COMPUTACION EN LA NUBE: DISEÑO DE UNA GUIA DE ADOPCION APLICANDO ELEMENTOS DE GESTION Y GOBIERNO DE TI

JOSE CARLOS VENDRIES RAMIREZ

Proyecto de Grado para optar por el Título de Magister en Gobierno de Tecnología Informática

Tutor:
JORGE ALBERTO GIL PEÑALOZA
MSc, MBA

FUNDACION UNIVERSIDAD DEL NORTE
DIVISION DE INGENIERIAS
MAESTRIA EN GOBIERNO DE TECNOLOGIAS DE INFORMACION
BARRANQUILLA
2015

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Barranquilla, 13 de enero de 2015

DEDICATORIA

A mis padres y hermano.

A mi esposa e hijos.

AGRADECIMIENTOS

A Dios y a la Santísima Virgen María por permitirme realizar bajo su guía permanente el presente proyecto.

A Jorge Alberto Gil Peñaloza, MSc, MBA**,** Tutor del Proyecto, por su asesoría y dedicación en la formulación, desarrollo y revisión del proyecto.

A mi esposa e hijos por su apoyo, comprensión y tiempo para poder desarrollar el proyecto.

CONTENIDO

pág

LISTA DE FIGURAS

RESUMEN

El presente proyecto de grado presenta una problemática existente de gobierno y gestión de tecnología de información debido a la aparición de una tecnología disruptiva como es la computación en la nube, expone un marco teórico describiendo contextual y conceptualmente la computación en la nube, relaciona algunos estándares, normas y mejores prácticas de gobierno y gestión de tecnologías de información, plantea un marco metodológico compuesto de fases como guía para la adopción de computación en la nube y finalmente aplica alguna de sus fases en un caso práctico.

1. FORMULACION DEL PROBLEMA

1.1 ANTECEDENTES DE LA PROBLEMÁTICA A ABORDAR.

Las dependencias de tecnología de la información en las empresas han presentado diferentes esquemas de operación en el tiempo, de acuerdo con sus intereses particulares. Entre ellas:

Recursos propios: realizar todas las actividades con recursos propios.

Tercerización de TI: contratar con terceros algunas de las funciones de TI. (Outsourcing de TI – ITO)

Tercerización de procesos de TI: contratar con terceros procesos de TI completos (Subconjunto de Outsourcing de procesos de negocio BPO)

Tercerización en otros países: contratar funciones que son realizadas en otros países (Offshorig)

Híbrido: mezcla de los esquemas anteriores.

Cada esquema generó una ampliación de servicios, desde alternativas parciales como alquilar un espacio en centros de cómputo de terceros, o alquilar capacidades de cómputo, hasta el suministro de bienes por demanda con administración completa de los mismos. Adicionalmente, el desarrollo y ampliación de las comunicaciones acompañada de disminución de costos de los servicios relacionados, la evolución de los servicios administrados y los adelantos en virtualización dieron paso a nuevos servicios surgiendo así la computación en la nube.

El Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology) (NIST) de los EE. UU. define la computación en la nube como "un modelo para habilitar un cómodo acceso en red omnipresente, a solicitud, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, recursos de almacenamiento, aplicaciones y servicios) que se puede conformar y proveer rápidamente con un esfuerzo administrativo mínimo o una interacción mínima con el proveedor de servicios"

Por otra parte, independiente de los esquemas de operación, los departamentos de Tecnologías de la información, tienen como retos principales mantener los servicios de TI disponibles, reducir costos, enfocarse en actividades de valor para el negocio, administrar la complejidad de su operación, alinear TI con los objetivos de negocio incrementar la eficiencia y efectividad, acceder a personal de TI calificados, reducir tiempos de entrega de servicios, ejercer control, ofrecer

servicios seguros y cumplir con la regulación existente. Todo esto dentro de un marco de gestión y gobierno de TI.

La computación en la nube es una alternativa para los departamentos de TI para entregar sus servicios a la empresa, pero su adopción debería considerar si se cumple o no con los retos mencionados.

1.2 PLANTEAMIENTO

La computación en la nube está cambiando la forma de hacer negocios. Pocos esquemas o tecnologías han sido adoptados tan rápidamente principalmente por sus ofrecimientos de bajo costo, rápida implementación y mayor eficiencia.

Sin embargo, en concepto del autor de este trabajo las empresas deberían evaluar si la computación en la nube aplica para su realidad en particular, si entrega los beneficios que se promulgan sin exponer a la empresa a riesgos y si los procesos de Gobierno y gestión de TI deberían adaptarse al modelo de servicio elegido.

¿Como hacer esa evaluación, como adoptar la computación en la nube cumpliendo los requisitos de seguridad, de mitigación de riesgos, de gestión de costos y de control? Estos son cuestionamientos que dan origen a este proyecto de grado.

1.3 DESCRIPCION

La computación en la nube es una alternativa utilizada por muchas empresas y la tendencia de su uso está en crecimiento. Su adopción no libera a las dependencias de tecnologías de información de sus responsabilidades de Gobierno y gestión de los riesgos financieros, de cumplimiento y de seguridad que implica, por lo que se requiere que las empresas establezcan un direccionamiento alineado con la estrategia de negocio y la aplicación de prácticas de gobierno y gestión para el manejo de los mismos, a ser empleados durante su adopción.

Las Empresas desconocen las respuestas a preguntas como:

- Qué es la computación en la nube?
- Cuáles son sus características?
- Qué modelos de servicio existen?,
- Qué modelos de implementación hay?
- Cuáles son los beneficios?
- Cuáles son los riesgos?
- Qué controles pueden disminuir el riesgo

- Qué costos iniciales existen?
- Qué costos recurrentes hay?
- Cómo se evalúan los servicios?
- Cómo se adapta el sistema de Gestión y Gobierno de TI?
- Cómo adoptar la computación en la nube?

Antes de emprender el camino hacia la computación en la nube, las empresas deberían dar respuesta estas preguntas.

1.4 JUSTIFICACION

El mercado de servicios de computación en la nube está en aumento y las empresas requieren evaluar la adopción de servicios basados computación en la nube.

Adoptar computación en la nube sin evaluar o evaluar mal puede llevar a las empresas a ampliar sus riesgos, aumentar sus costos y a exponer la seguridad de su información en lugar de reducir los riesgos, disminuir los costos y asegurar su información.

Una guía metodológica puede ayudar a las empresas a adoptar o rechazar la computación en la nube con base en criterios y argumentos cualitativos, preservando que las funciones de TI se mantengan dentro de un marco ge Gestión y Gobierno de TI.

Así como la computación en la nube es novedosa, de utilidad para las empresas, una guía de adopción también lo es y su realización es viable con una metodología adecuada.

2. OBJETIVOS

2.1 GENERAL

Desarrollar una guía para la adopción de computación en la nube dentro de un marco de gestión y gobierno de tecnología de información que permita considerar los riesgos asociados a esta tendencia tecnológica

2.2 OBJETIVOS ESPECIFICOS

- Descripción de un marco conceptual para unificar definiciones, conceptos, alrededor de la computación en la nube
- Establecimiento de un marco contextual que describa la situación actual de la computación en la nube.
- Exploración de elementos en las normas, estándares y mejores prácticas seleccionando los conceptos que aplicarían en cuanto a su relación con la computación en la nube: Gobierno y Gestión (COBIT), Riesgo (ISO 31000), Seguridad (ISO 27000).
- Estructuración de la guía de adopción.
- Aplicación parcial a un caso particular del marco metodológico propuesto.

2.3 ALCANCE Y LIMITACIONES

El resultado del trabajo es una guía genérica en el contexto actual de la tecnología y de servicios de computación en la nube. No pretende ser una norma, un estándar o mejor práctica, por el contrario busca mostrar que se pueden aplicar elementos de diferentes normas, estándares y mejores prácticas en la adopción de una tendencia tecnológica en un estado particular, como es la computación en la nube.

3. METODOLOGIA EMPLEADA

Se desarrollarán los siguientes pasos metodológicos:

1. Presentación del marco teórico y estado del arte de la computación en la nube.
2. Presentación de normas, estándares y mejores prácticas aplicables a la gestión de y gobierno de TI, en especial aquellos asociados a la administración y tratamiento de riesgos producto de la adopción de nuevas tendencias y filosofías tecnológicas.
3. Construcción de un marco metodológico compuesto por fases, con entradas y salidas esperadas producto de la ejecución de cada una de ellas.
4. Aplicación parcial del marco metodológico como trabajo de campo en alguna organización.

4. MARCO TEORICO

4.1 COMPUTACION EN LA NUBE

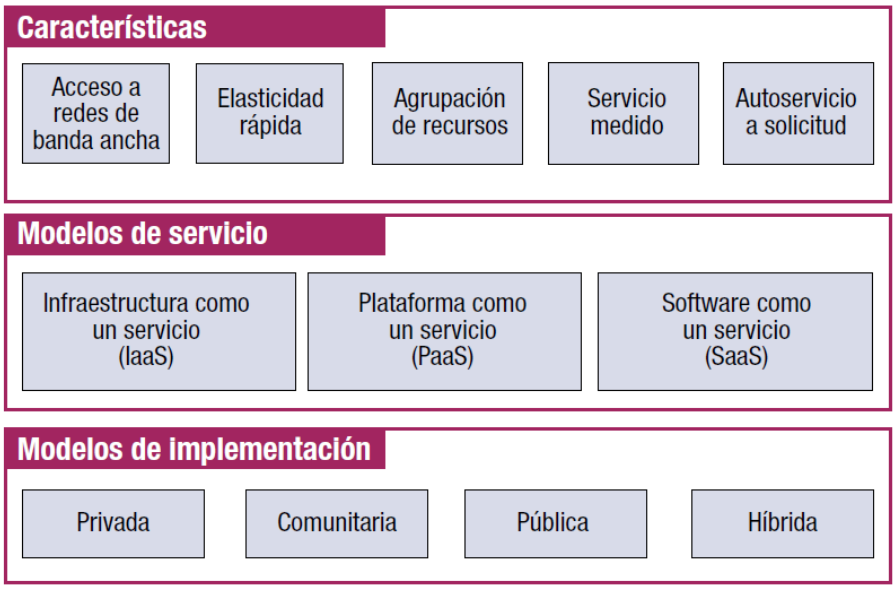
4.1.1 Definición

El Instituto Nacional de Normas y Tecnología de los Estados Unidos, NIST por sus siglas en inglés, (National Institute of Standards and Technology - NIST) define la computación en la nube como

> "Un modelo para habilitar un cómodo acceso en red omnipresente, a solicitud, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, recursos de almacenamiento, aplicaciones y servicios) que se puede conformar y proveer rápidamente con un esfuerzo administrativo mínimo o una interacción mínima con el proveedor de servicios"[1]

El NIST propone un modelo compuesto por 5 características, tres modelos de servicio y cuatro modelos de implementación:

Figura 1. Características de Computación en la nube[2]



[1] Mell, Peter; Timothy Grance; US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, The NIST Definition of Cloud Computing, NIST, USA., 2011 citado en ISACA. Calcular el ROI de la nube: Desde la perspectiva del cliente. USA.2013. p. 6

[2] Ibid.

4.1.2 Características

El modelo de computación en la nube descrito por el Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology -NIST) de los Estados Unidos tiene las siguientes características[3]:

4.1.2.1 Acceso a redes de banda ancha

De acuerdo con el NIST, debe ser posible acceder a la red en la nube a través de mecanismos estándares que promueven el uso en diferentes plataformas, ya sea un computador personal de escritorio o portátil, una tableta, un teléfono inteligente, un dispositivo móvil.

Esto implica un reto para los países y los proveedores de servicios de telecomunicaciones que deberían tener una cobertura de servicios con una alta capacidad y también un reto para las empresas que deberían poseer redes internas y servicios con terceros de buena capacidad.

Por otra parte se requiere establecer una política de gobierno de movilidad que regule el uso de todos los dispositivos, incluyendo aquellos que los empleados traen a la oficina

4.1.2.2 Elasticidad rápida

Según el NIST, el suministro de capacidad debe ser rápido y elástico para facilitar una rápida expansión o una rápida contracción de las capacidades contratadas en cualquier momento. Para el cliente, las capacidades disponibles para aprovisionar aparecen a menudo ilimitadas.

4.1.2.3 Agrupación de recursos

El proveedor agrupa sus recursos informáticos (como almacenamiento, procesamiento, memoria, ancho de banda, máquinas virtuales) para prestar servicios a diversos clientes utilizando un modelo de múltiples usuarios (Multitenant), con diferentes recursos físicos y virtuales, en diferentes sitios geográficos, atendiendo por demanda de forma dinámica las solicitudes de asignación y reasignación. Existe un sentido de independencia geográfica.

[3] Mell, Peter; Timothy Grance. US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, The NIST Definition of Cloud Computing, NIST,USA. 2011. P 2.

Por otra parte, el cliente no tiene control o no sabe exactamente donde están los recursos que le proporciona el proveedor Se puede acordar una ubicación a nivel de país, región, centro de datos

4.1.2.4 Servicio Medido

Los sistemas en la nube se ofrecen utilizando una métrica de referencia, por ejemplo, capacidad de almacenamiento, procesamiento, ancho de banda, número de cuentas de usuario activas, número de empleados. De esta manera se controla y optimiza el uso de recursos de manera automática

Los clientes y proveedores tienen una medida acordada para monitorear, controlar y analizar reportes del servicio.

4.1.2.5 Autoservicio a solicitud

El proveedor de la nube debe poder suministrar, capacidades de computación, de manera automática, sin requerir interacción humana con cada proveedor de servicio.

4.1.3 Modelos de servicio

El NIST propone 3 modelos de servicio que se describen a continuación: Software como servicio (SaaS), Plataforma como servicio (PaaS) e Infraestructura como servicio (PaaS)[4]

4.1.3.1 Software como servicio (SaaS)

La capacidad que recibe el cliente es la utilización de las aplicaciones del proveedor que se ejecutan en la infraestructura de la nube. El cliente accede a las aplicaciones desde diferentes dispositivos cliente a través de una interfaz de cliente ligero (thin client), como un explorador web o a través de programas interfaces.

La administración y el control de la infraestructura de nube (Redes, servidores, Sistemas operativos, almacenamiento) y de las capacidades de la aplicación individual las realiza el proveedor

[4] Ibid. P 2-3.

4.1.3.2 Plataforma como servicio (PaaS)

La capacidad que recibe el cliente es la utilización de la infraestructura de nube del proveedor para desplegar aplicaciones adquiridas o desarrolladas por el cliente utilizando lenguajes de programación, librerías, servicios soportados por el proveedor.

La administración y el control de la infraestructura de nube (red, servidores, sistemas operativos o almacenamiento) son realizadas por el proveedor. El cliente tiene control sobre las aplicaciones desarrolladas y posiblemente ajustes de configuraciones para el ambiente que hospeda la aplicación.

4.1.3.3 Infraestructura como servicio (IaaS)

La capacidad que recibe el cliente es la posibilidad de implementar software arbitrario, incluyendo sistemas operativos y aplicaciones sobre la infraestructura de nube del Proveedor (Redes, almacenamiento, Servidores)

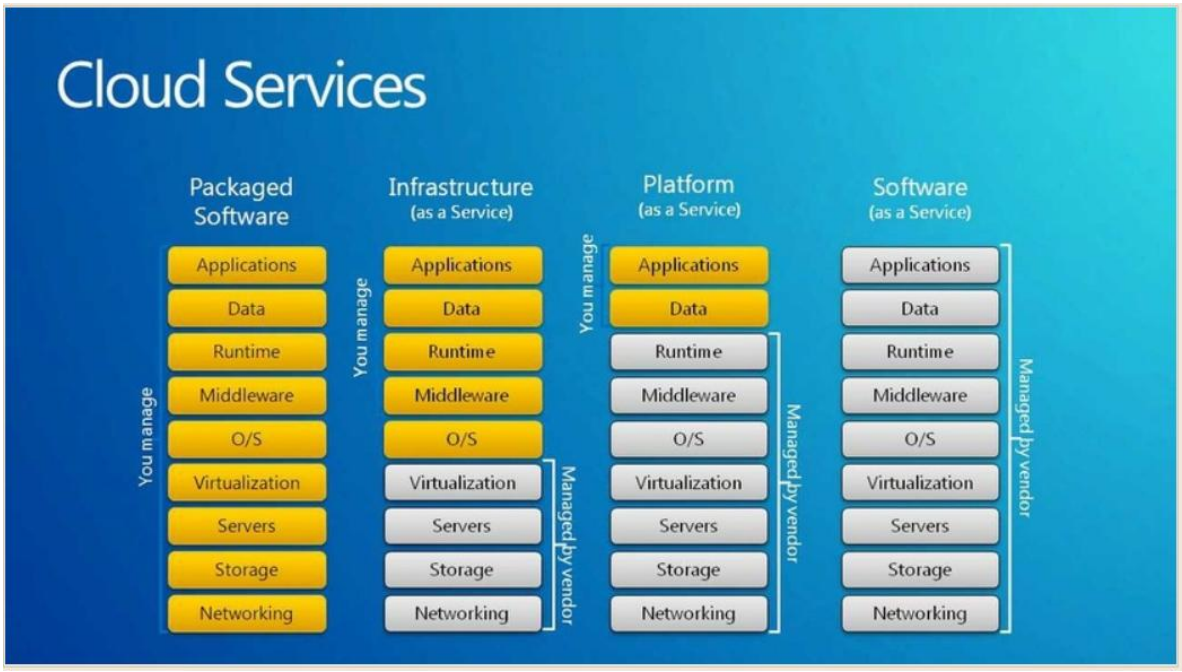
El cliente tiene control sobre aplicaciones desplegadas, sistemas operativos y posiblemente control limitado sobre componentes de red.

4.1.3.4 Comparación de los modelos de servicio

La siguiente figura compara los modelos de servicio, destacando las responsabilidades que están a cargo del Proveedor y a cargo del cliente en cada modelo

Figura 2 Comparación de los modelos de servicio[5]

[5] KLU Cloud Computing Seminar. [En línea] India, KLU University, Disponible en internet: http://klucloudseminar.weebly.com/



4.1.4 Modelos de despliegue

El NIST propone 4 modelos de despliegue: Nube privada, Nube comunitaria, Nube pública y Nube híbrida, que se describen a continuación[6]:

4.1.4.1 Nube Privada

La infraestructura de nube es provisionada para el uso exclusivo de de una organización. Puede ser gestionada, operada y ser propiedad de una organización, un tercero o combinación. Puede existir dentro o fuera de la organización.

4.1.4.2 Nube comunitaria

La infraestructura de nube es provisionada para el uso exclusivo de una comunidad de consumidores de organizaciones que han compartido intereses. Puede ser propiedad de, manejada y operada por una o más organizaciones en la comunidad, un tercero o una combinación de ellos. Puede existir dentro o fuera de la organización.

[6] Mell, Timothy. Op. cit. . P 3.

4.1.4.3 Nube pública

La infraestructura de nube es aprovisionada para uso abierto por el público en general. Puede ser propiedad, manejada y operada por una organización de negocios, académica, de gobierno, o combinaciones de ellas. Existe dentro del sitio del proveedor de nube.

4.1.4.4 Nube híbrida

La infraestructura de nube es la composición de dos o más infraestructuras de nube (privada, comunitaria o pública) que continúan siendo entidades únicas, pero que están unidas mediante tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones (por ejemplo, ampliación de la nube [cloud bursting] para equilibrar la carga entre las nubes.)

4.1.5 Estado de la computación en la Nube

La computación en la nube es una realidad. En esta sección se presentarán diferentes noticias, estudios, tendencias de la computación en la nube de diferentes fuentes.

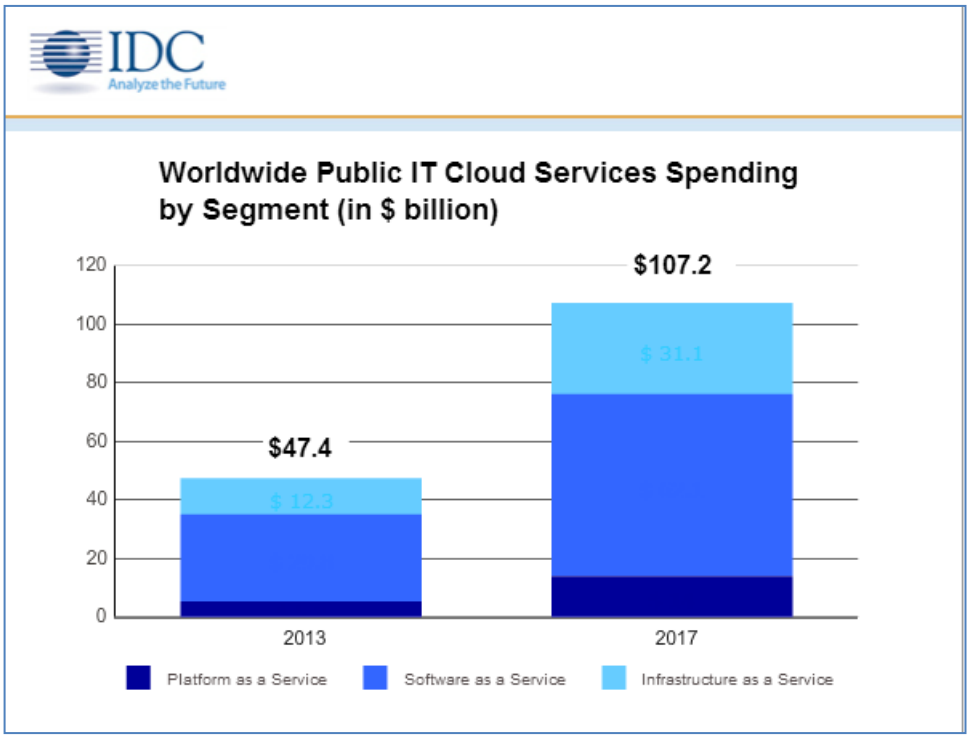
4.1.5.1 Según IDC[7]

IDC proyectó que para el 2017 la inversión en servicios de de TI de Nube pública alcanzará USD 107 billones de dólares frente a los 47.4 billones del 2013 con una tasa de crecimiento anual de 23.5%. La computación en la nube es un habilitador de cambios en la forma como las compañías consumen y usan la información y va a haber un paso hacia otra escala de adopción, mucho más grande y mayor orientada a soluciones y usuarios. La primera ola estuvo enfocada en incrementar la eficiencia de los departamentos de TI, en los siguientes años el foco será la innovación en la medida que las compañías inviertan en computación en la nube para apoyar sus ofrecimientos competitivos. La aparición de nubes privadas virtuales (VPC) con los atributos de nubes públicas y las características de control y privacidad de las nubes privadas favorecerán su utilización.

La siguiente figura muestra el Gasto en servicios de nube IT pública a nivel mundial (en billones de USD)

[7] IDC. Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast (Doc #242464)" [en línea]. Disponible en: Internet: http://www.idc.com/getdoc.jsp?containerId=242464

Figura 3 Gasto en servicios de nube IT pública a nivel mundial (en billones de USD)



El documento completo "Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast (Doc #242464)" está disponible en http://www.idc.com/getdoc.jsp?containerId=242464

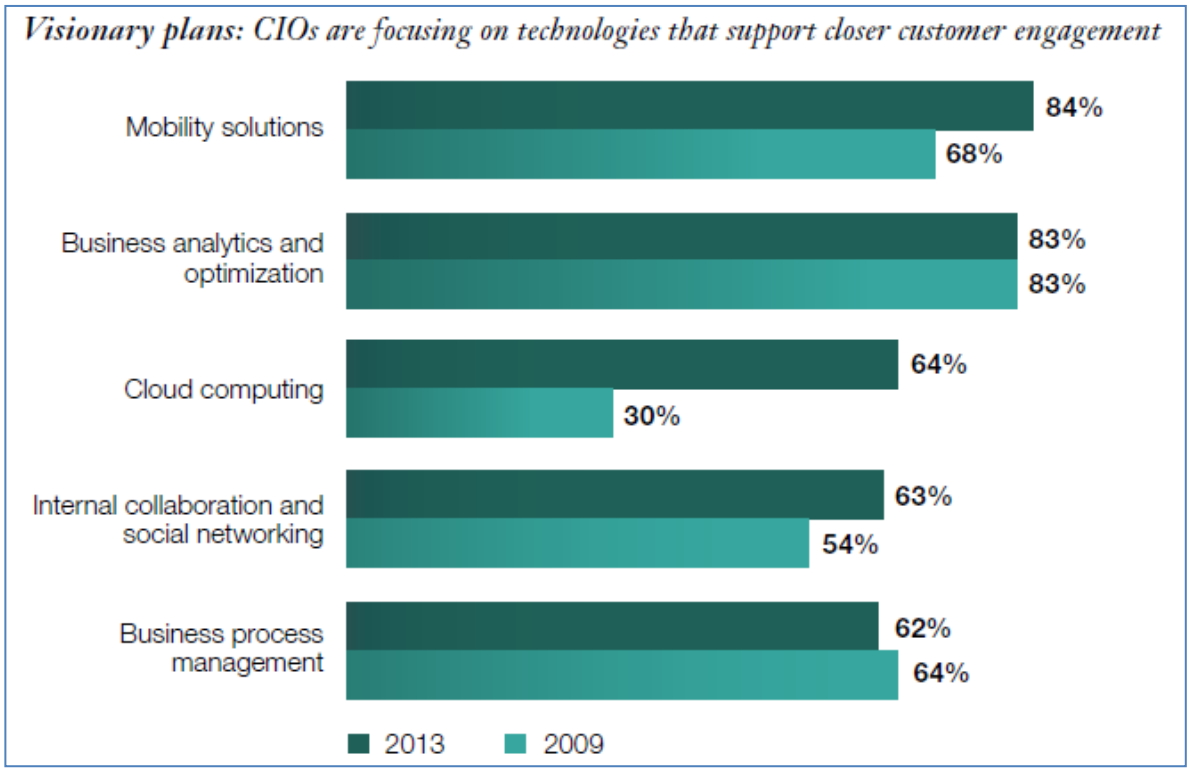
4.1.5.2 Según IBM [8]

En el 2013, IBM entrevistó 16256 Directores de TI para saber como estaban ayudando a sus empresas para ser Activados en clientes.

- La computación en la nube es una tecnología crucial para compromiso con los clientes (30% en 2009).
- 64% de los encuestados se enfocan en soluciones móviles
- 64% en soluciones de computación en la nube

[8] IBM. Moving from the backoffice to the front lines. [en línea]. Estados Unidos. 2013. Disponible en: Internet: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03580USEN

Figura 4 CIOs enfocados en tecnologías que soportan compromiso con clientes



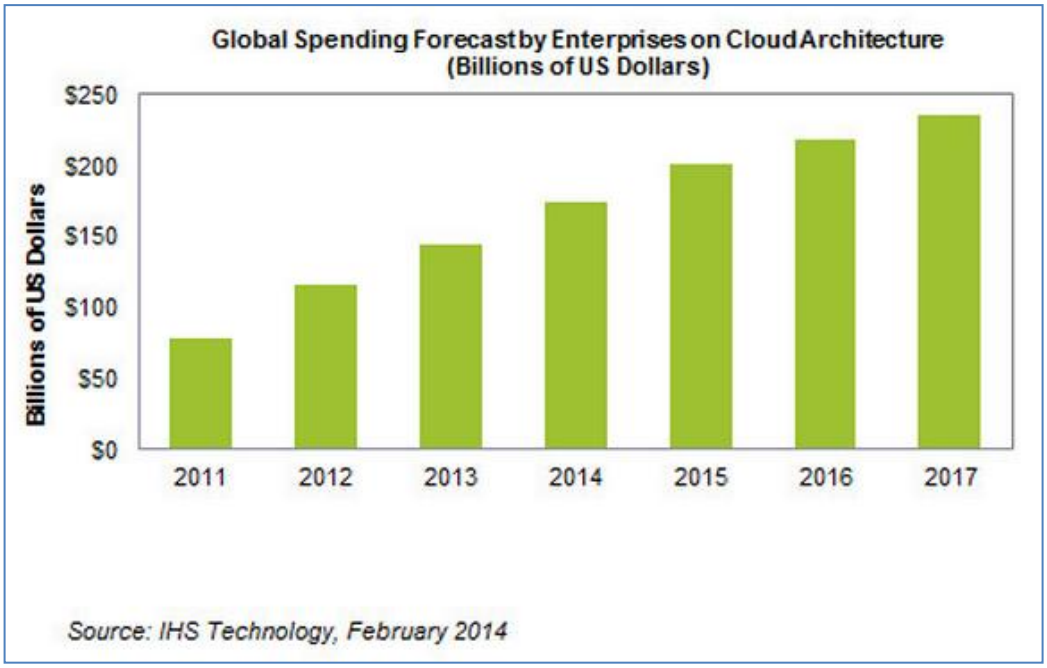
4.1.5.3 Según IHS

IHS es la líder fuente global de información crítica proporcionando datos confiables y completos y experiencia a negocios y gobiernos alrededor del mundo.

IHS en su reporte “The cloud: redefining the information, Communication and technology industry” estima que los gastos de negocios globales para infraestructura y servicios relacionados con la nube alcanzaran los 174.2 billones de dólares de Estados Unidos en el 2014 y en 235.1 billones en el 2017

Con la nube tocando cada consumidor y empresa alrededor del mundo, gasto relacionado con la nube en almacenamiento, servidores, aplicaciones y contenido será dedicado a construir un marco de trabajo que sea rápidamente escalable, altamente dinámico, disponible bajo demanda y que requiera mínima gestión.

Figura 5 Tendencias de gastos globales por empresas en arquitectura cloud



El reporte completo se puede consultar en https://technology.ihs.com/445918/cloud-big-data-report-a-paradigm-shift-in-the-ict-industry-2013

4.1.5.4 Según Centaur Partners

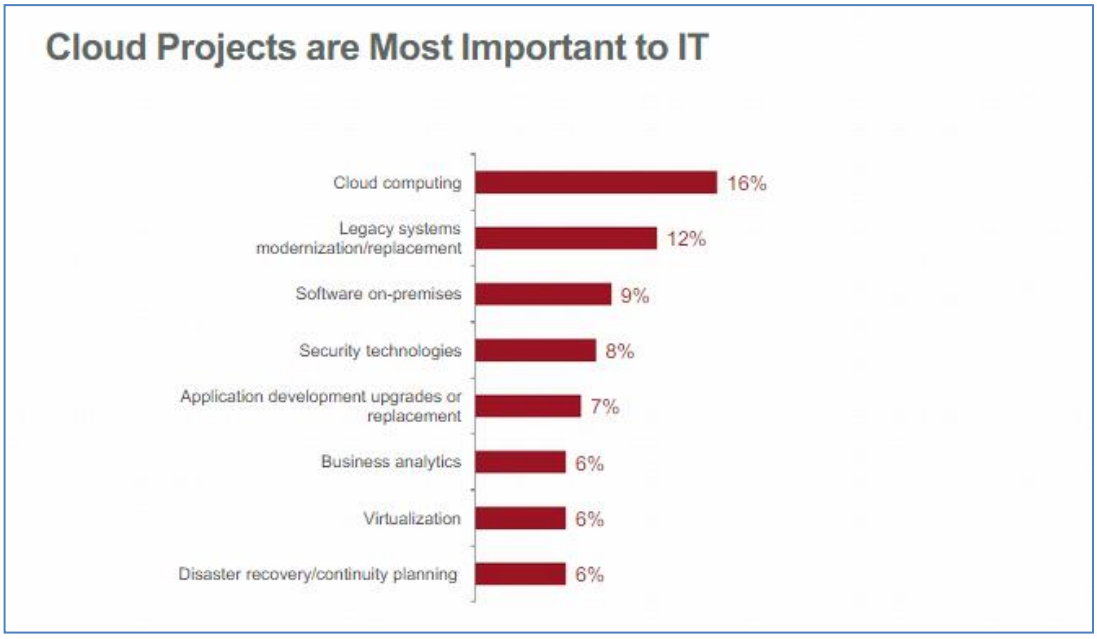
Centaur Partner en su reporte “SaaS Market overview” de febrero de 2014 predice que el total de ingresos de SaaS saltará del un 10% del total mercado de software empresarial en el 2010 hasta un 16% en el 2016 y predice que los ingresos de servicios de aplicaciones de negocio basadas en la nube crecerán de USD13.5 B en el 2011 a USD32.8 B en el 2016

El reporte completo está disponible en https://technology.ihs.com/445918/cloud-big-data-report-a-paradigm-shift-in-the-ict-industry-2013

4.1.5.5 Según Computerworld

Computerworld en su estudio “Computerworld Forecast Study 2015” indica que el 16% de los participantes consideran los proyectos de cloud computing más importantes para TI frente a 9% para Software en Sitio

Figura 6 Proyectos en la Nube son más importantes para TI



Y en su estudio “Computerworld state of the Enterprise” del 2 de marzo de 2014 indica que hay un compromiso en invertir en tecnologías emergentes como Computación en la nube y que un 41% de empresas están explorando o experimentando con computación en la nube, 18 usan parcialmente, 24% están obteniendo beneficios. Y a 16% no la están usando.

Ambos estudios están disponibles en http://www.computerworldmediakit.com/research.html

Figura 7 Nube continua siendo foco de Inversión

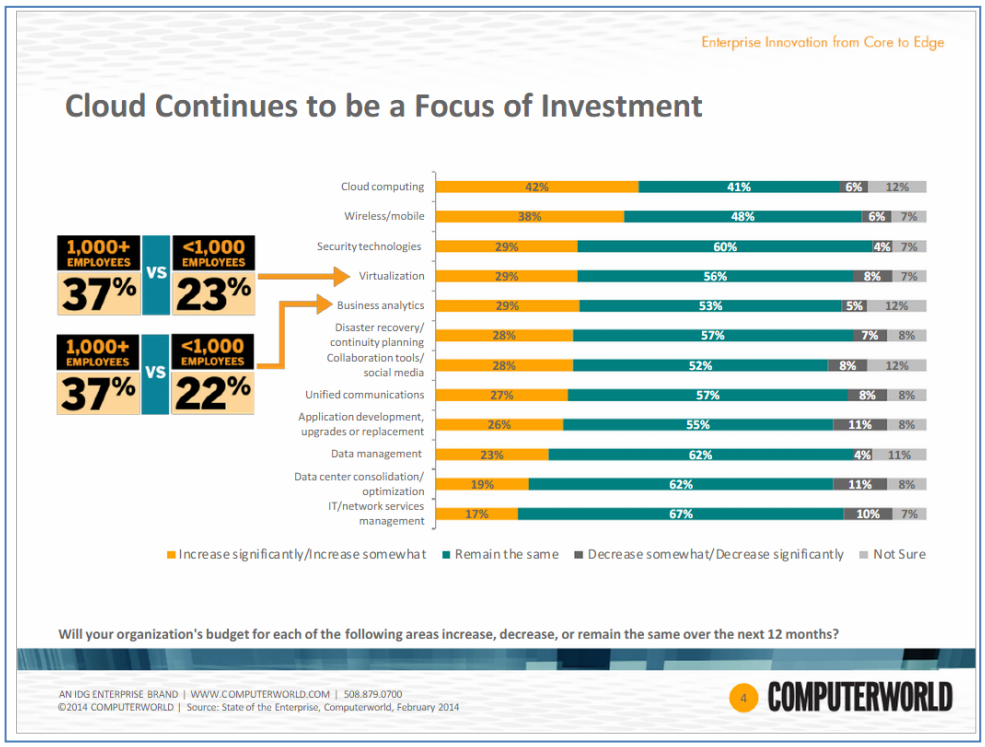
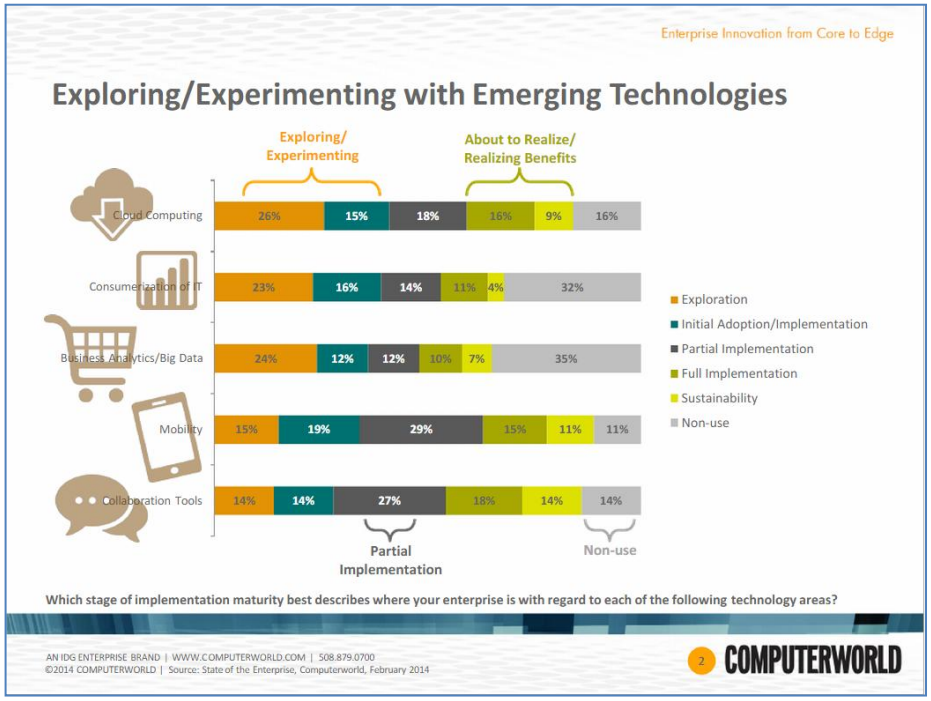


Figura 8 Explorando Experimentando con tecnologías emergentes



4.1.5.6 En Colombia[9] [10]

Las empresas Avanxo y Position Comunicaciones publicaron en el 2013 la segunda edición del Estudio Nacional de tendencias de Cloud Computing en Colombia

Las principales conclusiones de este estudio fueron:

- Se entrevistaron a 800 directivos de TI
- La computación en la nube deja de ser exclusiva para empresas visionarias
- 8% manifestó que invertirían más de 500 millones en el siguiente año
- 43% manifestó que invertirían entre 50 y 500 millones de pesos en el siguiente año
- Los servicios en la nube que pensaban migrar eran mensajería/colaboración (50,4%), Infraestructura (44,2%), CRM (20,4%), Inteligencia de negocios (19,5%)
- El sector de consumo masivo es el que presenta mayor adopción de computación en la nube y el sector gobierno e industria el que menor
- Solo 5% de las empresas más grandes No estaba contemplando migrar a la nube soluciones de negocio
- El 72% de las empresas eligen proveedores con recursos locales, 69% elige proveedores con caso dé éxito en Colombia
- El aumento de las conexiones de banda ancha en Colombia y las políticas de movilidad lideradas por el Ministerio de Tecnologías de la Información y las Comunicaciones, seguirán contribuyendo a la adopción de la computación en la nube.

[9] Las empresas colombianas se suben a la nube. [en línea] disponible en internet: http://avanxo.com/estudio.html

[10] Resultados del estudio nacional de tendencias de adopción de Cloud computing y nuevas tecnologías. 2013. . [en línea] disponible en internet: http://cintel.org.co/wp-content/uploads/2013/06/resultados-del-estudio.pdf

4.2 NORMAS, ESTANDARES Y MEJORES PRÁCTICAS DE GOBIERNO DE TI Y LA COMPUTACION EN LA NUBE

El modelo de computación en la nube debería ser gobernado y gestionado como parte del Gobierno y Gestión de TI. Bajo esta perspectiva las Normas, los estándares y los marcos de trabajo actuales, pueden ser aplicados para gobernar y gestionar en la nube.

Debido a la rápida y amplia aceptación del modelo de computación en la nube, y los retos que plantea, se están presentando extensiones, guías complementarías, adaptaciones que tratan en forma específica a la nube, dentro del marco general de TI.

Se presenta a continuación una descripción general de normas, estándares y marcos de trabajo que pueden servir de referencia para el gobierno y gestión de la computación en la nube, teniendo como referencia Gobierno y Gestión de TI, Seguridad y Riesgo. No es el objetivo realizar una presentación detallada, ni desarrollar cada uno de los componentes. El lector interesado puede acudir a los documentos oficiales y profundizar según el nivel de detalle que desee y consultar otros marcos de trabajo, estándares o normas no citados aquí.

4.2.1 COBIT

COBIT® Objetivos de Control para la Información y la Tecnología relacionada, es un marco de trabajo integral ampliamente aceptado con una evolución y madurez obtenida durante alrededor de 15 años gracias al aporte de la comunidad de profesionales que conforman la entidad ISACA.

Las empresas se apoyan en COBIT® como ayuda para alcanzar sus objetivos de gobierno y la gestión de las TI corporativas

COBIT® brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica.

- Reúne el Consenso de los expertos.
- Enfocadas fuertemente en el control y menos en la ejecución.
- Ayudan a optimizar las inversiones habilitadas por TI, aseguran la entrega del servicio y brindan una medida contra la cual juzgar cuando las cosas no vayan bien.

A continuación se presenta una descripción general de COBIT y los productos que lo componen.

4.2.1.1 Un poco de Historia

Desde sus inicios COBIT® ha tenido una orientación hacia los negocios. La entidad que promovió su desarrollo fue la ISACF (Information Systems Audit and Control Foundation), diseñando un producto para los profesionales dedicados a las actividades de control. En 1995 se emprendió el proyecto que produce su primera edición en 1996

En abril de 1998 se publica la edición 2 de COBIT™ que mejora el respecto a la primera edición, suministrando un mayor número de documentos de referencia, gerenciales y más objetivos de control

La misión del COBIT era: buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.[11]

En Julio de 2000, el comité directivo de COBIT y Instituto de Gobierno de TI (IT Gobernante Institute™ publican la versión 3, con un enfoque en Gestión.

La cuarta edición fue publicada en el 2005 (4.0), y en 2007 (4.1) con un enfoque de Gobierno de TI. En el 2008 se publica ValIT 2.0 y en el 2009 RiskIT.

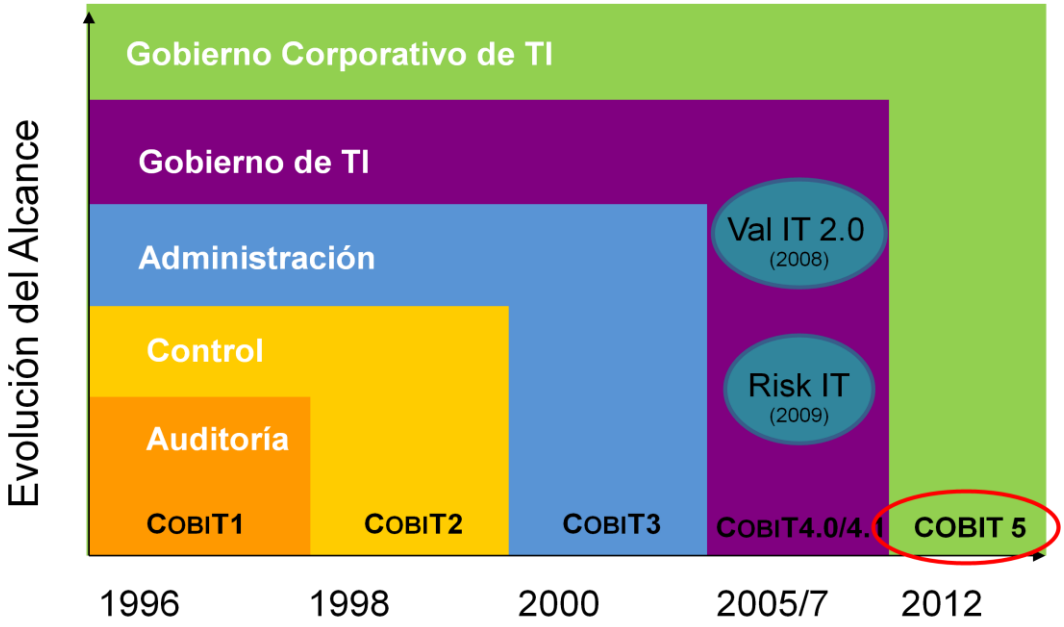
La versión 5 es publicada en el 2012 por ISACA con un enfoque en Gobierno Corporativo de TI y Gestión, siendo un marco de trabajo completo.

Con más de 115,000 integrantes en 180 países, ISACA® (www.isaca.org) ayuda a empresas y líderes de TI a construir confianza en y maximizar el valor de la información y de los sistemas de información. Fundada en 1969, ISACA es una fuente confiable de conocimiento, estándares, comunidad, y desarrollo de carrera para los profesionales en gobierno, privacidad, riesgos, seguridad, aseguramiento y auditoría de sistemas (ISACA)[12]

La siguiente figura muestra la evolución de COBIT desde su primera versión en 1966. Ha pasado de un enfoque en auditoría a un enfoque de Gobierno corporativo de TI, de unos pocos documentos a un conjunto extensos de publicaciones

[11] Information Systems Audit and Control Foundation. Cobit Resumen Ejecutivo. Abril de 1998. 2da. Edición. P 1..
[12] Disponible en http://www.isaca.org/spanish/Pages/default.aspx

Figura 9 Evolución de COBIT



4.2.1.2 Componentes de COBIT 5

COBIT5 proporciona un marco integral que ayuda a las Empresas a lograr sus metas y a entregar valor mediante un gobierno y una administración efectivos de las Tecnologías de Información.

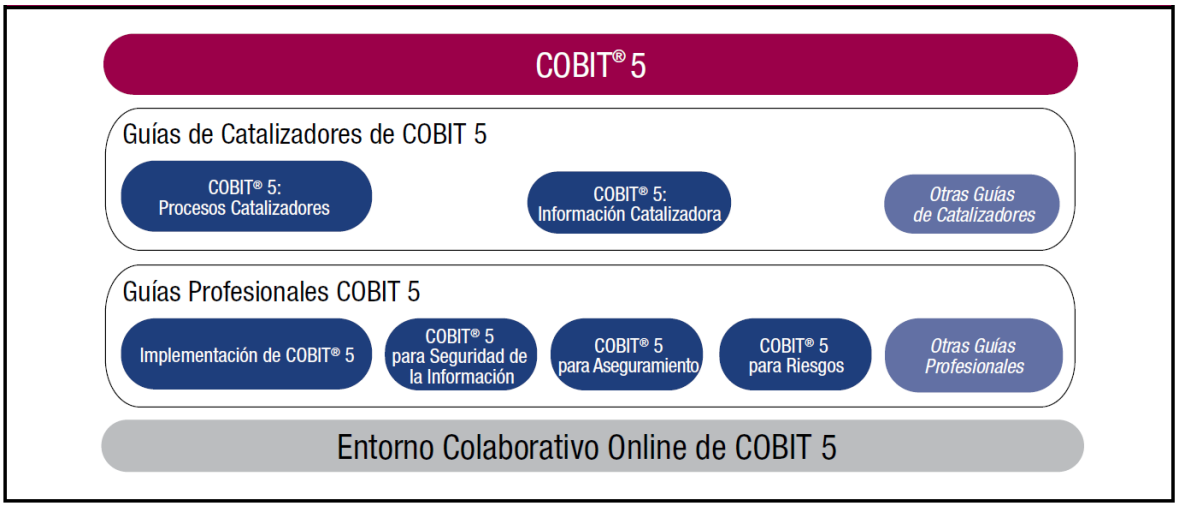
COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas[13].

COBIT 5 es una familia de Productos basada en 5 cinco principios y siete habilitadores, compuesta por diferentes publicaciones, algunas ya desarrolladas, otras en desarrollo y otras por desarrollar en un futuro. Los Productos están disponibles en diferentes idiomas para facilitar su divulgación y uso internacional.

La siguiente figura resume la familia de productos COBIT 5:

[13] ISACA. COBIT® 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Quinta Edición. Estados Unidos, 2012. . P 13

Figura 10 Familia de Productos COBIT 5[14]



A continuación se indica la finalidad de los productos:

- COBIT 5 (el marco de trabajo)

La publicación COBIT 5 contiene el marco COBIT 5 para el gobierno y la gestión de las TI de la empresa.

El documento presenta una visión general de COBIT, la descripción de los 5 principios, una guía de implementación, y el modelo de capacidad de los procesos de COBIT

Contiene también anexos que relacionan las metas de la empresa con las metas de TI, Mapeo de las Metas de TI con los Procesos de TI, las necesidades empresariales y un mapeo de COBIT con otros estándares

- Guías de catalizadores de COBIT 5

En estas guías se discuten en detalle los catalizadores para el gobierno y gestión, estas incluyen:

- COBIT 5: Procesos Catalizadores [15]

[14] Ibid. P 11
[15] ISACA. COBIT® 5 Procesos Catalizadores.. Quinta Edición. Estados Unidos, 2012

COBIT 5: Procesos Catalizadores complementa al Marco de Trabajo COBIT 5 y contiene una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de referencia de COBIT.

Es una herramienta para quien desee profundizar en detalles el modelo de procesos de COBIT y los 37 procesos que lo componen.

Al final del documento se incluyen apéndices que contienen comparación con los procesos de COBIT 4.1, Val IT 2.0 y Risk IT y comparación de las metas Corporativas – Metas de TI –Procesos de TI

- COBIT 5: Información Habilitadora [16]

Esta publicación soporta y extiende el Marco de trabajo COBIT 5, enfocándose en la información habilitadora (o catalizadora o Posibilitadora). El documento cubre los atributos del modelo de información y el ciclo de vida, introducidos en el documento COBIT 5 Marco de trabajo.

Es una guía de referencia para obtener un pensamiento estructurado sobre la información y su gobierno y gestión, el cual puede ser aplicado a través del ciclo de vida de la información, desde su concepción y diseño, pasando la construcción de sistemas de información, la seguridad y aseguramiento hasta el uso y disposición de ella.

- Otras guías de catalizadores

Otras guías de catalizadores están disponibles en www.isaca.org/cobit

- <u>Guías profesionales de COBIT 5:</u>

- COBIT 5 Implementación [17]

COBIT 5 Implementación complementa COBIT 5. El objetivo de esta guía de referencia es proveer un enfoque de buenas prácticas a la hora de implementar GEIT basado en un ciclo de vida de mejora continua que debe adaptarse a las Necesidades específicas de la empresa.

[16] ISACA. COBIT® 5 Enabling Information.. United States of America, 2013..
[17] ISACA. COBIT® 5 Implementación. Quinta Edición. Estados Unidos, 2012. P 9

El documento se enfoca en que la información y las tecnologías de información relacionadas, están en toda la empresa y que no es posible, ni es una buena práctica, separar los negocios y las actividades de TI relacionadas , por lo que el gobierno y la gestión TI de la empresa deberían implementarse como una parte integral del gobierno corporativo,

- COBIT 5 para Seguridad de la Información

Publicación en desarrollo, actualmente se encuentra disponible un preliminar. Proporciona guía para ayudar a los profesionales de seguridad y de TI a entender, utilizar, implementar y dirigir actividades relacionadas con seguridad de la información. Este documento es una evolución estratégica de COBIT 5 e incorpora los últimos pensamientos en Gobierno Corporativo y técnicas de gestión y entrega principios aceptados globalmente, prácticas, herramientas analíticas y modelos para ayudar a incrementar la confianza y valor de los sistemas de información[18]

- COBIT 5 para Aseguramiento

Guía diseñada para habilitar el desarrollo eficiente y efectivo de las iniciativas de aseguramiento, proporcionando direccionamiento en planeación, alcance, ejecución y seguimiento de revisiones de aseguramiento utilizando una hoja de ruta basada en aproximaciones de aseguramiento bien aceptadas.[19]

En desarrollo, disponible en versión preliminar.

- COBIT 5 para Riesgos

Este guía proporciona direccionamiento en cómo usar el Marco de trabajo COBT 5 para establecer funciones de gestión y gobierno de riesgo para la empresa. Es un acercamiento estructurado para usar los principios COBIT 5 para gobernar y gestionar el riesgo.[20]

En desarrollo, disponible en versión preliminar.

- Otras guías profesionales

Otras guías están disponibles en www.isaca.org/cobit

[18] ISACA. COBIT® 5 for information security (Preview). United States of America, 2012.. P. 2
[19] ISACA. COBIT® 5 for Assurance (Preview).. United States of America, 2013. P 2
[20] ISACA. COBIT® 5 for Risk (Preview).. United States of America, 2013.. p 1

- COBIT Online

Es una iniciativa de ISACA cuyo primer objetivo es proporcionar acceso fácil a las versiones en línea de las publicaciones de Cobit 5. Entorno colaborativo en línea, Disponible para dar soporte en el uso de COBIT 5. Ofrece un arreglo robusto de recursos de contenido y herramientas para avanzar en la gestión y gobierno de TI corporativo.

4.2.2 ISO 27000

La familia de normas ISO 27000 es un referente para la seguridad de información: la confidencialidad, Integridad, Disponibilidad, Autenticidad, Responsabilidad, No negación y Confiabilidad son atributos que buscan preservarse al gestionar información.

El uso de la familia de estándares permite a las organizaciones administrar la seguridad de los activos de información

A continuación se presenta una descripción general de las normas ISO 27000, partiendo de los primeros documentos que con el tiempo llegaron a ser parte de la familia de normas 27000 actuales

4.2.2.1 Un poco de Historia[21]

El origen de las normas 27000 actuales se remonta al Gobierno del Reino Unido, donde el Departamento de Industria y Comercio a través del CCSC (Commercial Computer Security Centre) generó el documento ITSEC con criterios de evaluación de seguridad para productos de seguridad de TI y el documento PD0003 código de buenas prácticas para la seguridad de la información. Esto hacia el año 1993.

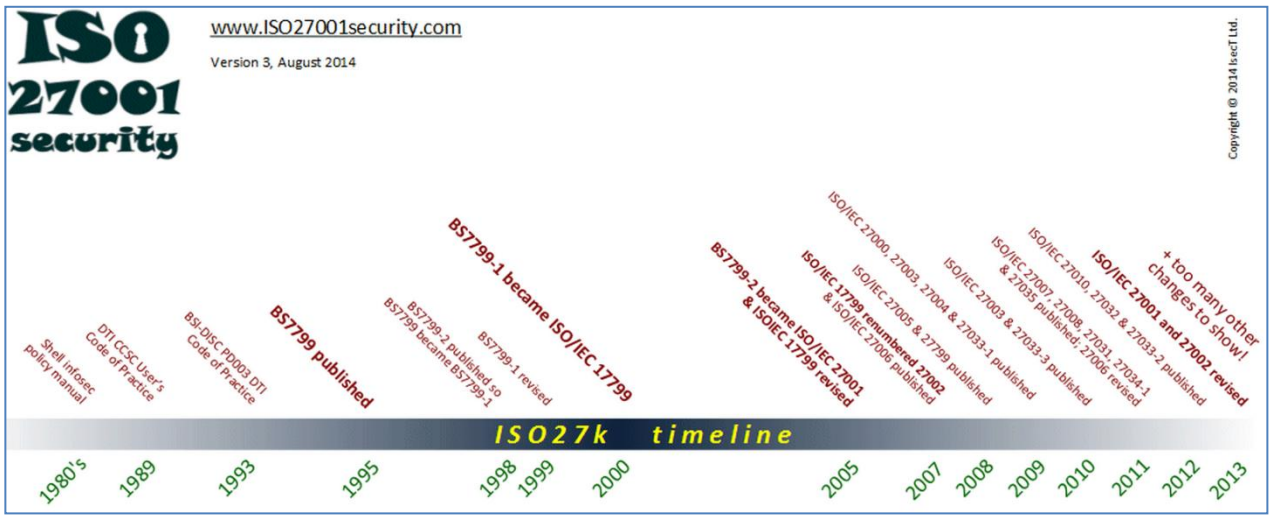
El PD0003 evolucionó bajo el Instituto de Estándares Británico, BSI por sus siglas en Ingles en el BS7779-1995. En 1998 el BSI publicó el BS7779-2 Sistema de Gestión de Seguridad de la información y e BS7799 se convirtió en BS-7799-1

[21] The ISO Directory. A Short History of the ISO 27000 Standards. [En línea]. Disponible en internet: http://www.27000.org/thepast.htm

Posteriormente el BS7779-1 fue desarrollado por la Organización Internacional para la Estandarización, por sus siglas en Inglés ISO (International Organization for Standardization) y se convirtió en ISO 17799-2000, ISO 17799:2005, ISO 27002:2007, ISO 27002:2013.

Por otra parte, el BS7799-2 se convirtió en ISO-27001:2005, ISO-27001.-2013.

Figura 11 Línea de tiempo ISO 27000[22]



4.2.2.2 Principales componentes de ISO 27000[23]

- ISO 27000

Proporciona descripción, vocabulario y relaciones de la familia de normas que tratan los Sistemas de Gestión de Seguridad de la Información (SGSI). La versión más reciente es de 2014.

- ISO 27001

Contiene los requisitos para establecer, implementar, Operar, verificar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) formal

[22] ISO 27k timeline. [en línea]. Disponible en: Internet: http://www.iso27001security.com/ISO27k_timeline.gif.

[23] BORTNIK, Sebastián. La serie de normas ISO 27000. [en línea]. USA. Publicado el 16 de abril de 2010. Disponible en internet: http://www.welivesecurity.com/la-es/2010/04/16/la-serie-de-normas-iso-27000/

dentro de un contexto de negocio. Especifica los requisitos para implementar y operar los controles de la seguridad. Es norma certificable. Incluye los requisitos de la ISO 17799 como anexo. La versión más reciente es la ISO/IEC 27001:2013 que reemplazó la ISO/IEC: 2005. Es de las normas más populares y utilizada por diferentes empresas en todo el mundo.

- ISO 27002

Es un código de buenas prácticas para la realización de un Sistema de Gestión de Seguridad de la Información (SGSI). Establece pautas y principios generales para definir, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). Entrega un catálogo de controles no obligatorios que apoyan desplegar con éxito un SGSI basado en ISO 27001

Está dividida en once dominios y en cada uno de ellos se destacan cuáles son las mejores prácticas o los controles recomendados para dar seguridad en la organización. Esta norma no es certificable. Su versión más reciente es la del 2013.

- ISO 27003

Es un apoyo a la norma 27001. Incluye directivas prácticas para la implementación de un Sistema de Gestión de Seguridad de la Información. Fue publicada en febrero de 2010.

- ISO 27004

Proporciona métricas que permiten determinar la eficacia del Sistema de Gestión de la seguridad de la información, de los objetivos de control y de los controles establecidos. Publicada en diciembre de 2009.

- ISO 27005

Dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona técnicas y metodología para evaluar y tratar los riesgos. Fue publicada en junio de 2008.

- ISO 27006

Especifica los requisitos de acreditación utilizados para acreditar las organizaciones de certificación en ISO 27001

- ISO/IEC 27017.

Tecnología de la información – Técnicas de seguridad - Código de práctica para controles de seguridad de la información basados en ISO 27002 para servicios en la nube (en desarrollo),

El estándar proporcionará guía de seguridad para proveedores de servicios en la nuble y clientes de estos servicios

- ISO/IEC 27018.

Tecnología de la información – Técnicas de seguridad. Código de práctica para protección de información identificable personal (PII Personally Identifiable Information) en nubes públicas actuando como PII processors.

Proporciona una guía para asegurar que los proveedores de servicio de nube ofrecen controles de seguridad de la información para proteger la privacidad de sus clientes. Pretende ser un referente para la selección de controles para protección de datos personales

- Otras normas ISO 27x [24][25]

- ISO/IEC 27007:2011 Tecnología de la información – Técnicas de seguridad. Guía para auditar los Sistema de Gestión de Seguridad de la Información (SGSI)
- ISO/IEC TR 27008:2011 Tecnología de la información – Técnicas de seguridad. Guía para auditores en controles de seguridad de la información

[24] About the ISO Estándard http://www.iso27001security.com/html/iso27000.html
[25] Disponible en www.iso.org

- ISO/IEC CD 27009 guía para aquellos que producen estándares para aplicación de ISO 27000 en sectores específicos. En desarrollo
- ISO/IEC 27010:2012 Tecnología de la información – Técnicas de seguridad. Proporciona guía en gestión de seguridad de la información para comunicaciones interorganizacionales e intersectores
- ISO/IEC 27011:2008 Tecnología de la información – Técnicas de seguridad. Guía de gestión de seguridad de la información para organizaciones de telecomunicaciones basada en ISO/IEC 27002
- ISO/IEC 27013:2012 Tecnología de la información – Técnicas de seguridad. Guía para la implementación conjunta de ISO/27001 e ISO/IEC 20000-1 Gestión de servicios
- ISO/IEC 27014:2013 Tecnología de la información – Técnicas de seguridad. Gobierno de Seguridad de la información
- ISO/IEC TR 27015:2012 Tecnología de la información – Técnicas de seguridad Guía en gestión de seguridad de la información para servicios financieros.
- ISO/IEC TR 27016:2014 Tecnología de la información – Técnicas de seguridad. Cubre economía en la gestión de seguridad de la información
- ISO/IEC TR 27019:2013 Tecnología de información – Técnicas de seguridad Guías de gestión de seguridad de la información basada en ISO/IEC 27002 para sistemas de control para procesos, específica para la industria de energía y servicios públicos (utilities)
- ISO/IEC NP 27021 explica las competencias y conocimientos requeridos por profesionales de gestión de la seguridad de la información (En desarrollo)
- ISO/IEC TR 27023 propone un mapeo de las versiones 20005 y 2013 de la 27001 y 27002.
- ISO/IEC 27031:2011 Tecnología de información – Técnicas de seguridad -- Guía para tecnología de comunicación e información preparación de continuidad del negocio
- ISO/IEC 27032:2012 Tecnología de información – Técnicas de seguridad. Guía para ciber seguridad.
- ISO/IEC 27033:2009+ Seguridad de la red.
- ISO/IEC 27034:2011 Tecnología de información – Técnicas de seguridad Guía para seguridad de aplicaciones
- ISO/IEC 27035:2011. Tecnología de información – Técnicas de seguridad Gestión de incidentes seguridad de información.
- ISO/IEC 27036:2013 Tecnología de información – Técnicas de seguridad. Seguridad de la información para relaciones con proveedores. Parte 3 Guía para la seguridad de tecnología de información y comunicación en la cadena de suministro

- ISO/IEC 27037:2012 Tecnología de información – Técnicas de seguridad Guías para identificación, recolección, adquisición, y preservación de la a evidencia digital.
- ISO/IEC 27038:2014 Tecnología de información – Técnicas de seguridad especificación para redacción digital
- ISO/IEC 27039 se preocupará de sistemas de prevención y detección de intrusos

4.2.3 ISO 31000

La norma ISO 31000 Gestión del Riesgo. Principios y Directrices., es un referente para las organizaciones de cualquier tipo, o dependencias de esas organizaciones, como es el caso de TI, para gestionar los riesgos.

La adopción de la computación en la nube puede afectar a las organizaciones con impactos económicos, normativos, operativos, por lo que manejar el riesgo efectivamente ayudará a TI y a la organización a desempeñarse en un ambiente de incertidumbre.

A continuación se presenta una descripción general de de la familia ISO 31000

4.2.3.1 Un poco de Historia

El estándar Australiano, Neozelandés AS/NZS 4360 fue publicado en 1995 basado en los conceptos de gestión del riesgo de la época. Una edición mejorada fue publicada en 1999 incluyendo elementos de consulta y comunicación. Después de casi 10 años, aparece la edición 2004 que consolidó apéndices y removió algunos de ellos hacia otros documentos.

En Colombia, La norma técnica Colombiana de gestión del riesgo 5254 es una traducción idéntica de la norma técnica Australiana AS/NZ 4360:2004

En el año 2009 se publica la ISO 31000 junto con la guía 73 aplicable y adaptable a un amplio rango de organizaciones e individuos. El concepto de riesgo se modifica incluyendo efectos positivos.

En Colombia se publica la NTC 31000 en el 2001 equivalente a la ISO 31000

4.2.3.2 Principales componentes de ISO 31000

- ISO 31000:2009 Gestión de Riesgo. Principios y Directrices[26] [27]

Esta norma proporciona principios y directrices genéricas en gestión de riesgo. Puede ser utilizada por cualquier empresa pública o privada, asociaciones, grupos o individuos y no es específica para algún sector o industria. No promueve uniformidad de gestión de riesgo en las organizaciones

La norma puede ser aplicada en un amplio rango de actividades, incluyendo estrategia, decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos y a cualquier tipo de riesgo independiente de su naturaleza y su efecto (positivo o negativo)

No hay certificaciones de la norma ISO 31000: 2009, pero proporciona guía para auditorías internas y externas.

En Colombia la norma es la NTC ISO 31000 la cual fue el remplazo de la norma NTC 5254, que en su prefacio establece "que tiene como objetivo proporcionar un marco genérico para establecer el contexto, identificación el análisis, el tratamiento, el seguimiento y la comunicación del riesgo" y que debería leerse en conjunto con otras normas aplicables.

La norma incluye términos y definiciones, describe los principios del riesgo y desarrolla el marco de referencia y el proceso de Gestión del riesgo.

Su utilización puede ayudar a las organizaciones, y áreas de TI a cumplir sus objetivos mejorando la identificación de oportunidades y amenazas y asignar efectivamente recursos para tratar el riesgo.

[26] INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. ISO 31000:2009 Risk Management:Principios and Guidelines: Abstract. [en línea]. Disponible en: Internet:: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170

[27] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION (ICONTEC). Gestión del riesgo: Principios y Directrices. NTC-ISO 31000. Bogotá: El instituto, 2011. 12 p

- ISO/TR 31004:2013 Gestión de Riesgo. Guía de implementación de ISO 31000[28]

Este documento proporciona una guía para las organizaciones para manejar el riesgo efectivamente mediante la implementación de ISO 31000

Similar a la ISO 31000, la ISO/TR 31004 no es específica a alguna industria o sector y puede ser utilizada por cualquier organización pública o privada, asociación, grupo o individuos y ser aplicada a cualquier parte de la organización

Si la empresa está buscando una guía de los conceptos, principios y marco de trabajo incluidos en la ISO 31000, una publicación de consulta es la ISO/TR 31004

- ISO Guide 73:2009 Gestión de Riesgo. Vocabulario[29]

Esta guía proporciona las definiciones de los términos genéricos relacionados con la Gestión de Riesgo. El documento ayuda a utilizar una terminología uniforme en los procesos, marco de trabajos relacionados con la gestión de riesgo. Su utilización facilita un entendimiento consistente y coherente para quienes trabajan en el manejo de riesgo.

- IEC 31010:2009 Gestión de Riesgo. Técnicas de valoración de riesgo[30]

Proporciona una guía en la selección y aplicación de técnicas sistemática para valoración de riesgo. No es certificable y no trata específicamente temas de seguridad para los que remite a la publicación ISO / IEC Guía 51

[28] INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. ISO 31004:2013 Risk Management: Guidance for the implementation of ISO 31000: Abstract. [en línea]. Disponible en: Internet: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56610

[29] INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. ISO Guidance 73:2009 Risk Management: Vocabulary: Abstract. [en línea]. Disponible en Internet: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44651

[30] INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. IEC 31010:2009 Risk Management: Risk Assessment techniques. [en línea]. Disponible en Internet: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51073

4.2.4 Otras Normas

4.2.4.1 PMBOK GUIA Y ESTÁNDARES

Los estándares globales del Project Management Institute proporcionan directrices y reglas a la gestión de Proyectos. En la adopción de la computación en la nube hay proyectos, y en estos proyectos la Guía del PMBOK es de utilidad.

Los estándares fundamentales son: Guía de los fundamentos para la dirección de proyectos (Guía del PMBOOK), el estándar para Gestión de programas, estándar para Gestión de portafolio y Modelo de madurez de gestión de proyectos organizacionales

4.2.4.2 COSO

El Committee of Sponsoring Organizations of the Treadway Commission (COSO), es una iniciativa privada de inco organizaciones, que desarrolla marcos de trabajo y directrices en gestión de riesgos, control interno y reducción de fraudes.

El comité ha publicado COSO Gestión de riesgo para la computación en la nube, Marco de trabajo integrado, documento que establece un lenguaje común y los fundamentos para las organizaciones para valorar y supervisar riesgo con una perspectiva de conjunto. Este marco de trabajo facilita la identificación de riesgos y de estrategias de mitigación relacionados con la evolución de la computación en la nube

5. MARCO METODOLOGICO PROPUESTO

Como resultado de este trabajo se puede afirmar que la adopción de computación en la nube es evolutiva, no hay un solo camino para llegar, pero cualquiera de ellos es extenso, lleno de retos y dificultades, pero también de logros y beneficios. No hay una regla del dedo pulgar de la mano derecha.

No obstante, este trabajo propone a continuación un marco metodológico compuesto de fases, las cuales pueden aplicar en algunos casos, en otros no, en algunos escenarios prácticos podrán ser suficientes, pero en otros limitadas. No es un marco de trabajo, son pasos metodológicos, una guía de adopción.

El lector podrá seleccionar y ajustar las fases de acuerdo con su interés particular y aplicar los marcos de trabajo que la guía referencia y complementar con otras que aquí no se indican.

5.1 FASE 1. ESTADO ACTUAL

El estado actual de la Gestión y gobierno de TI en la organización debería servir de referencia y punto de partida cuando se desee adoptar una nueva tecnología. La computación en la nube debería cumplir los requisitos actuales y los deseados por la organización.

Es posible que para proyectos pequeños de bajo impacto en la organización, esta fase pueda obviarse, sin embargo, es recomendable realizarla por primera vez, también como parte del ciclo de mejoramiento continúo de la organización. Cualquier proyecto, por pequeño que sea debería estar controlado y centralizado en TI.

Los siguientes elementos, pueden mostrar el contexto de Gestión y Gobierno de TI al iniciar el movimiento hacia una nueva forma de prestación de servicios de TI:

- Plan estratégico de la Organización
- Plan Estratégico de TI
- Políticas de TI
- Procesos de TI
- Procedimientos de TI
- Estructura organizacional de TI
- Modelo de Operación
- Niveles de acuerdos de Operación (interno)
- Nivel de apoyo del grupo directivo
- Arquetipo de toma de decisiones
- Requerimientos de Control y Cumplimiento
- Mapa de riesgos de la Organización

- Mapa de riesgos de TI (alineados con los de la organización)
- Modelo de Seguridad de TI

Si alguno de estos elementos están ausentes, no significa que se debe abortar la exploración de la Computación en la nube, pero la presencia parcial o total de un marco de Gobierno de de TI facilitará en proceso y permitirá una mejor alineación y operación de TI con el negocio.

Esta fase preliminar obtiene como resultado el contexto de Gobierno y Gestión de TI en la organización y los niveles de Gestión de Riesgo de ella.

5.2 FASE 2. LA ORGANIZACIÓN Y LA NUBE

El objetivo de esta fase es que la organización conozca las características de la computación en la nube, identifique las diferencias con los esquemas tradicionales de operación junto con el impacto de esas diferencias, identifique los riesgos genéricos de adopción de ella y establezca una posición respecto a la Computación en la nube

Los directivos de la organización junto con las dependencias de TI establecen el norte y definen claramente los beneficios y riesgos de la organización al adoptar la computación en la nube.

La computación en la nube no es un proyecto, no es un sustituto, debería ser vista como parte de la estrategia de la organización para apalancar el logro de los objetivos de ella.

Como resultado de esta fase la organización tendrá elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI. En las siguientes fases, de acuerdo con el caso específico, podrán usarse como referencia estos lineamientos generales.

La organización debería establecer los siguientes elementos, sin limitarse a ellos.

5.2.1 Identificación de las características y modelos de nube

Utilizar la información ampliamente aceptada sobre computación en la nube, para conocer sus características, modelos de servicio (IaaS, PaaS, SaaS) y modelos de despliegue (pública, Comunitaria, Privada e Híbrida)

La organización debería tener claridad sobre lo que es Computación en la nube y lo que no es.

5.2.2 Identificación de diferencias con enfoque tradicional

Identificar las diferencias entre el enfoque tradicional de operación de TI y la Computación en la nube, además del impacto de estas diferencias sobre la forma de gobernar, gestionar, monitorear y controlar la adquisición y el uso de la tecnología

Generalmente se define y revisa la computación en la nube sobre lo que es y no sobre cómo funciona. Para la áreas de TI los cambios en el cómo generan cambios en la forma de gestionar y gobernar recursos de TI

5.2.3 Identificación de los beneficios esperados

Se ha divulgado que la computación en la nube trae beneficios a las organizaciones entre ellos agilidad, disminución de costos, sinergias al compartir recursos, escalabilidad, confiabilidad.

La organización debería identificar los beneficios genéricos y cuáles de ellos le aplican y son de su interés.

5.2.4 Identificación de riesgos

Se identifican riesgos comunes a los diferentes Modelos de servicio y diferentes modelos de despliegue con sus tratamientos para disminuir los impactos.

Posteriormente, se identifican riesgos genéricos y específicos de cada modelo de servicio y de cada modelo de despliegue con sus tratamientos para disminuir los impactos.

En caso que la Organización posea una gestión de riesgos formal, con un mapa de riesgos definido, se puede hacer una comparación con los riesgos genéricos de la nube para obtener un sub conjunto de riesgos y tratamientos más ajustado a la organización.

Al finalizar la sub fase, la Organización tendrá una herramienta con los riesgos asociados a cada modelo de servicio y despliegue, la que podrá utilizar en los diferentes proyectos de Computación en la nube que se formulen y que le permitirán identificar el modelo apropiado en cada caso y exigir a los proveedores de servicios unos requisitos precisos que disminuyan la exposición al riesgo para la organización.

5.2.5 Responsabilidades

La organización debería tener claridad hasta donde llega su responsabilidad y desde donde inicia la responsabilidad del proveedor de servicios.

Este cambio en los límites de responsabilidad genera cambios en los roles y responsabilidades dentro de la organización

5.2.6 Material de apoyo para esta fase

Además del marco teórico de este documento y las referencias allí citadas, se mencionan algunos documentos que pueden servir de apoyo para esta fase:

- CLOUD SECURITY ALLIANCE. Security Guidance for critical areas of focus in cloud computing. Versión 3.0. 2011. 177 p. [en línea]. Disponible en: Internet http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
- FARAHMAND, Fariborz. Risk perception and trust in cloud. Isaca Journal Volume 4, 2010. 8 p.
- ISACA. Gobierno en la nube: Preguntas que los consejos directivos deben formular. 2013. 9 p
- ISACA. Principios rectores para la adopción y el uso de la computación en la nube. Febrero, 2012. 16 P
- ISACA. Security considerations for cloud computing. 2012. 80 p. ISBN 978-60420-263-2

5.3 FASE 3 REQUERIMIENTOS

En esta fase se identifican y documentan los requerimientos funcionales y no funcionales (como los operativos, de seguridad, de control y cumplimiento) de una necesidad específica de la organización.

Como entrada para esta fase se utilizan

- El estado actual de la Gestión y gobierno de TI en la organización obtenido en la fase 1.
- Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI obtenidos en la fase 2 (Características de la Nube, diferencias con enfoques tradicionales, beneficios, Riesgos de cada modelo, Responsabilidades).

Los requerimientos sirven de entrada para la búsqueda de soluciones. Son la base para el documento de invitación a presentar ofertas, el cual a su vez es la base de un buen contrato.

Esta fase es similar a la identificación de requerimientos de otras tecnologías, pero más compleja ya que puede involucrar diferentes prestaciones informáticas. Si redactar un documento de requerimientos para una prestación específica presenta una dificultad y complejidad, redactarlo para varias prestaciones informáticas al tiempo tiene una dificultad y complejidad que es la suma de las dificultades y complejidades de cada una de ellas.

No se puede enfocar solo en la solución principal y dejar de lado lo que está alrededor de ella. Es común que los requerimientos de una solución en la nube pueden incluir elementos como el software, la arquitectura de desarrollo, capacidad de procesamiento, capacidad de almacenamiento, Base de datos, servidores, centro de datos, contingencia, comunicaciones, servidores, alta disponibilidad y procesos de recuperación ante desastres. Cada elemento tendrá un responsable en la organización, con sus requerimientos específicos.

Por otra parte, los requerimientos funcionales y no funcionales deberían estar alineados con los objetivos del negocio, para que la adopción de esta tecnología disruptiva sea más fácilmente justificada. Si es el primer proyecto, entre más apunte hacia la misión del negocio, más ganancias rápidas puede generar.

La organización debería identificar y documentar que busca, que desea, que requiere.

Como resultado de esta fase se obtiene un documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización.

Se utiliza el término “específico”, porque la guía se puede aplicar en diferentes momentos, siendo las fases 1 y 2 genéricas y de la fase 3 en adelante específicas para una necesidad en particular de la organización.

5.3.1 Material de apoyo para esta fase

Además del marco teórico de este documento y las referencias allí citadas, se mencionan algunos documentos que pueden servir de apoyo para esta fase:

- CASTIGLIONI, Fabio. CRUDELE Michele, Manage non-functional requirements for cloud applications: Software design patterns for PaaS environments. USA. IBM Corporation. 30 de Junio de 2014. 21 p

- COMGROUP, inc. Request for proposal template Hosted/Cloud Unified Communications and collaboration solution. Marzo 2013. 36 p
- DIMENSION DATA. IaaS Request for proposal template. Marzo 2, 2014.24p
- ISACA. Controls and Assurance in the cloud: Using COBIT 5. United States of America, 2014. 266 p. ISBN 978-1-60420-465-0

5.4 FASE 4 SELECCIÓN DEL MODELO DE SERVICO Y DESPLIEGUE DE COMPUTACION EN LA NUBE

El objetivo de esta fase es identificar el modelo de servicio de computación en la (IaaS, PaaS, SaaS) y el modelo de despliegue de computación en la nube (pública, Comunitaria, Privada e Híbrida), para requerimientos específicos de la organización

Como entrada para esta fase se utiliza:

- El estado actual de la Gestión y gobierno de TI en la organización obtenido en la fase 1
- Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI obtenidos en la fase 2 (Características de la Nube, diferencias con enfoques tradicionales, beneficios, Riesgos de cada modelo, Responsabilidades).
- Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización, obtenido en la fase 3.

Se utiliza el término “específico”, porque la guía se puede aplicar en diferentes momentos, siendo las fases 1 y 2 genéricas y de la fase 3 en adelante específicas para una necesidad en particular de la organización.

Cada organización dependiendo del nivel de estudio, conocimiento e información realizada, identificará el modelo que considere más apropiado a su necesidad, el cual debería ser analizado en forma específica en las siguientes fases. Una decisión no aplica para todas las empresas.

La evaluación del modelo de servicio contiene elementos más técnicos, mientras que el modelo de despliegue tiene consideraciones de riesgo.

En el caso del modelo de servicio, la decisión dependerá de consideraciones como si se está evaluando un solución para un proceso estándar (un CRM por ejemplo) en cuyo caso el camino hacia la nube será más viable que si la solución no es estándar (por ejemplo una aplicación para la repartición del impuesto de distribución de energía para la región sur de Colombia) o también si las soluciones

requieren comunicarse con otras soluciones o no (interfaces) o si el hardware es específico o no, o si el ambiente de desarrollo es propietario o estándar.

En el caso del modelo de despliegue, las consideraciones pueden incluir si los datos que se migran a la nube son sensibles / personales / críticos, si los procesos de negocio apoyados por la solución son críticos, si la demanda es predecible, si hay impedimentos legales, la jurisdicción legal, los niveles de servicio (ANS / SLA), temas de recuperación ante desastres y continuidad del negocio. Cada organización debe establecer sus propias preguntas y sus criterios de decisión.

Ejemplos de referencia de árbol de decisión del modelo de servicio y de despliegue en la nube se encuentra en el documento “Controls and Assurance in the cloud: Using COBIT 5.de ISACA.

Como resultado de esta fase se obtiene la identificación del modelo de servicio y el modelo de despliegue de computación en la nube para la solución específica buscada por la organización.

5.4.1 Material de apoyo para esta fase

Además del marco teórico de este documento y las referencias allí citadas, se mencionan algunos documentos que pueden servir de apoyo para esta fase.

- BADGER, Lee, et al. Cloud computing Synopsis and recommendations . National Institute of Standards and technology. NIST Special publication 800-146. USA, Mayo 2012. 81p ISACA. Controls and Assurance in the cloud: Using COBIT 5. United States of America, 2014.. 266 p.. ISBN 978-1-60420-465-0
- NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY (NIST). Technical considerations for USG Cloud Computing deployment Decisions. Fisrt working draft. USA, Noviembre 3, 2001. 90p
- TAPPER, David. GENS, Frank. Prepare and Assess readiness for cloud services. IDC..USA. March 2011. 13 p,
- THE OPEN GROUP. Jericho Forum Cloud Cube Model. USA. Abril 2009. 16 p

5.5 FASE 5. ANALISIS DE RIESGOS

El objetivo de esta fase es identificar los riesgos específicos y sus tratamientos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización.

Como entrada para esta fase se utiliza:

- El estado actual de la Gestión y gobierno de TI en la organización obtenido en la fase 1.
- Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI obtenidos en la fase 2 (Características de la Nube, diferencias con enfoques tradicionales, beneficios, Riesgos de cada modelo, Responsabilidades).
- Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización, obtenido en la fase 3.
- Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización, obtenidos en la fase 4.

Para el análisis de riesgos , la organización puede utilizar, si lo tiene establecido, su sistema de gestión de riesgo (ERM por sus siglas en inglés Enterprise risk management), o la norma de gestión de riesgos como la ISO 31000 o marcos de trabajo de riesgo, o COBIT, apoyándose en documentación existente sobre riesgos y controles para computación en la nube emitida por organizaciones como European network and information security agency (ENISA), Cloud security alliance (CSA), Open Web application security Project (OWASP).

Las listas pueden ser extensas, pero la organización debe ajustarlas a su contexto y necesidades específicas

Como resultado de esta fase se obtiene el análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización.

5.5.1 Material de apoyo para esta fase

Además del marco teórico de este documento, se mencionan algunos documentos que pueden servir de apoyo para esta fase.

- FARAHMAND, Fariborz. Risk perception and trust in cloud. Isaca Journal Volume 4, 2010. 8p
- ISACA. COBIT® 5 for Risk (Preview).. United States of America, 2013.. 19 p. ISBN 978-1-60420-340-0
- ISACA. Controls and Assurance in the cloud: Using COBIT 5. United States of America, 2014.. 266 p.. ISBN 978-1-60420-465-0
- MARSH. The cloud Risk framework: Informing decisions about moving to the cloud. United Kingdom. Mayo 2012. 20 p.
- SCHAEFER. Thomas. HOFMANN, et al. Selecting the right cloud operating model: Privacy and Data Security in the Cloud. Vol. 3, 2014. ISACA Journal

[En línea]. Disponible en internet: http://www.isaca.org/Journal/Past-Issues/2014/Volume-3/Documents/Selecting-the-Right-Cloud-Operating-Model_joa_Eng_0514.pdf

5.6 FASE 6 ANALISIS DE COSTOS

El objetivo de esta fase es analizar la viabilidad económica de la solución y modelo de servicio y despliegue específico seleccionado para atender los requerimientos formulados por la organización

Se utiliza el término específico, porque la guía se puede aplicar en diferentes momentos, siendo las fases 1 y 2 genéricas y de la fase 3 en adelante específicas para una necesidad en particular

Como entrada para esta fase se utiliza:

- El estado actual de la Gestión y gobierno de TI en la organización obtenido en la fase 1.
- Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI obtenidos en la fase 2 (Características de la Nube, diferencias con enfoques tradicionales, beneficios, Riesgos de cada modelo, Responsabilidades).
- Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización, obtenido en la fase 3.
- Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización, obtenidos en la fase 4.
- Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización, obtenido en la fase 5.

La organización puede aplicar el método financiero de evaluación que tenga establecido, Retorno de inversión (ROI por sus sigla en inglés, Costo total de propiedad (TCO por sus siglas en inglés), Valor presente neto (VPN), tasa interna de retorno (IRR por sus siglas en inglés), o periodo de retorno, o una combinación de ellos, ya que una sola herramienta puede que no ofrezca todos los elementos para una toma de decisión.

La mayor dificultad de esta fase es la obtención de datos. Es posible que no se tengan datos para comparar, ya sea por la estructura de costos de la organización o porque haya procesos que TI no realiza actualmente, pero que la solución si incluye. Cuando las organizaciones no consideran a TI como prestadora de servicios y no miden el costo de estos, sino que manejan valores globales de

operación, es difícil comparar con el valor de un servicio ofrecido por un tercero. Si la organización no posee alta disponibilidad pero la solicita como requisito en el servicio en la nube, no tiene valores de la operación interna para comparar con la propuesta del tercero. Por otra parte los beneficios y riesgos no son siempre cuantificables, por lo que el análisis económico puede ser incompleto o con un grado de incertidumbre.

Se recomienda que esta fase sea liderada por el departamento de Costos/Finanzas/inversiones de la organización con participación de los responsables de los procesos que se apoyaran con la solución en la nube y personal de informática.

Al finalizar la fase se obtendrá una recomendación de viabilidad o no viabilidad de la solución basada en computación en la nube que atiende los requerimientos específicos formulados por la organización.

5.6.1 Material de apoyo para esta fase

Además del marco teórico de este documento, se mencionan algunos documentos que pueden servir de apoyo para esta fase:.

- ISACA. Calcular el ROI de la nube: Desde la perspectiva del cliente. USA. Julio 2013. 17p
- ISACA. The Val IT framework 2.0
- MANN, Andi. MILNE Hurt. MORAIN Jeanne. How to calculate the advantages of a private cloud to make a business case. Searchcloudcomputing.com [En línea]. Disponible en internet http://www.bitpipe.com/detail/RES/1308681118_97.html 10p

5.7 FASE 7 SELECCIÓN DEL PROVEEDOR

El objetivo de esta fase es elegir el proveedor de la solución y modelo de servicio y despliegue específico seleccionado para atender los requerimientos específicos formulados por la organización

Como entrada para esta fase se utiliza:

- El estado actual de la Gestión y gobierno de TI en la organización obtenido en la fase 1.
- Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI obtenidos en la fase 2 (Características de la Nube, diferencias con enfoques tradicionales, beneficios, Riesgos de cada modelo, Responsabilidades).

- Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización, obtenido en la fase 3.
- Modelo de servicio y el modelo de despliegue de computación en la nube para la solución específica buscada por la organización, obtenidos en la fase 4.
- Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización, obtenido en la fase 5.
- La recomendación de viabilidad o no viabilidad de la solución basada en computación en la nube que atiende los requerimientos específicos formulados por la organización, obtenida en la fase 6.

.
En esta fase la organización puede utilizar sus procedimientos de compra de servicios utilizando el material particular obtenido en las fases previas, realizar las revisiones de cumplimiento respecto a lo solicitado y realizar la selección.

La organización puede encontrar escenarios donde el proveedor de la selección sea una entidad y el implementador sea otra empresa autorizada por el proveedor de la solución, por lo que se manejarán dos procesos de selección de proveedores con objetos diferentes. Esta situación debe considerarse en los pasos previos de esta guía.

Al finalizar la fase se obtendrá una recomendación de proveedor de la solución.

5.8 FASE 8 CONTRATACION

El objetivo de esta fase es obtener un documento de contratación que refleje los acuerdos entre las partes para la entrega de las prestaciones informáticas basadas en computación en la nube.

Como entrada para esta fase se utiliza:

- El estado actual de la Gestión y gobierno de TI en la organización obtenido en la fase 1.
- Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI obtenidos en la fase 2 (Características de la Nube, diferencias con enfoques tradicionales, beneficios, Riesgos de cada modelo, Responsabilidades).
- Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización, obtenido en la fase 3.

- Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización, obtenidos en la fase 4.
- Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización, obtenido en la fase 5.
- La recomendación de viabilidad o no viabilidad de la solución basada en computación en la nube que atiende los requerimientos específicos formulados por la organización, obtenida en la fase 6
- La recomendación del proveedor seleccionado en la fase 7.

Como se mencionó en fases previas, la computación en la nube involucra diferentes prestaciones, por lo que el contrato debería incluir las condiciones de cada una de ellas, con sus particularidades. Esto hace que el contrato sea complejo en su estructura, redacción y revisión.

La contratación de bienes y servicios informáticos ha presentado una dificultad y un reto para las dependencias jurídicas de las organizaciones porque no existen normativas jurídicas como ocurre en otros campos como por ejemplo un arrendamiento o una compra- venta de un bien inmueble. Cuando en una tecnología como la computación en la nube se involucra diferentes prestaciones tecnológicas, la complejidad del contrato aumenta. Por ejemplo, las partes tienen que acordar como regular temas de propiedad intelectual, de protección de datos personales, de diferentes marcos jurídicos según los países donde se contrate/preste el servicio y telecomunicaciones, entre otros.

Esta fase debería ser liderada por el departamento legal de la organización y podría tener el apoyo de firmas externas con experiencia en contratación de prestaciones informáticas, en particular en la nube. Se recomienda que quienes participen en esta fase revisen documentación acerca de contratación de computación en la nube para involucrar en el documento elementos que sirvan para manejar una relación contractual equitativa.

Las dependencias de TI deben apoyar esta fase entregando aquellos elementos desde la perspectiva de Tecnología de información que permitan regular los riesgos identificados en fases previas y faciliten la administración del servicio contratado.

Al finalizar la fase se obtendrá un documento revisado que regule la relación de Cliente – proveedor para la prestación de la solución de computación en la nube.

5.8.1 Material de apoyo para esta fase

Se mencionan algunos documentos, libros, artículos que pueden servir de apoyo para esta fase:

- ARENAS CORREA, José David. Estrategias de autorregulación en bienes intangibles: el caso del software. Universidad de Antioquia. Facultad de derecho y Ciencias políticas. Edición 2013. ISBN: 978-958-8790-84-8
- CITY OF LOS ANGELES. Contract No. C-116359. 2009-2014. [en línea]. Disponible en: Internet http://cityclerk.lacity.org/lacityclerkconnect/?fa=ccon.viewrecord&contractnum=C-116359
- McDONALD, Steve. Legal and Quasi-Legal Issues in Cloud Computing Contracts. [en línea]. Disponible en: Internet http://net.educause.edu/section_params/conf/CCW10/issues.pdf 4p
- TRAPPLER, Thomas. If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues. June, 25, 2010. . [en línea]. Disponible en: Internet http://www.educause.edu/ero/article/if-its-cloud-get-it-paper-cloud-computing-contract-issues
- VELASCO, Arean Hernando. El derecho informático y la gestión de la seguridad de la información: una perspectiva con base en la norma ISO 27001. Revista de derecho, Universidad del Norte, 29: 333-366, 2008
- TECHTARGET (Searchcloudsecurity). Cloud computing legal issues: Developing cloud computing contracts. . [en línea]. Disponible en: Internet http://searchcloudsecurity.techtarget.com/tutorial/Cloud-computing-legal-issues-Developing-cloud-computing-contracts

5.9 RESUMEN MARCO METODOLOGICO

A continuación se presenta un resumen de las fases presentadas en este capítulo, con las entradas y salidas esperadas producto de la ejecución de cada una de ellas.

Figura 12. Resumen del Marco Metodológico

ENTRADAS	FASE	SALIDAS
• Plan estratégico de la Organización • Plan Estratégico de TI • Políticas de TI • Procesos de TI • Procedimientos de TI • Estructura organizacional de TI • Modelo de Operación • Niveles de acuerdos de Operación (interno) • Nivel de apoyo del grupo directivo • Arquetipo de toma de decisiones • Requerimientos de Control y Cumplimiento • Mapa de riesgos de la Organización • Mapa de riesgos de TI (alineados con los de la organización) • Modelo de Seguridad de TI	**1. ESTADO ACTUAL**	1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización • Información sobre Nube : ISACA, European network and information security agency (ENISA), Cloud security alliance (CSA), Open Web application security Project (OWASP), National Institute of Standards and Technology (NIST), Foros	**2. LA ORGANIZACIÓN Y LA NUBE**	2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI: 2.1 Identificación de las características y modelos de nube 2.2 Identificación de diferencias con enfoque tradicional 2.3 Identificación de los beneficios esperados 2.4 Riesgos asociados a cada modelo de servicio y despliegue 2.5 Responsabilidades de la organización y de proveedor de Nube
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización 2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI	**3. REQUERIMIENTOS**	3. Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización 2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI 3. Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización	**4. SELECCIÓN DEL MODELO DE SERVICIO Y DESPLIEGUE DE COMPUTACION EN LA NUBE**	4. Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización 2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI 3. Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización 4. Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización	**5. ANÁLISIS DE RIESGOS**	5. Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización

ENTRADAS	FASE	SALIDAS
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización 2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI 3. Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización 4. Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización 5. Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización	**6. ANÁLISIS DE COSTOS**	6. Recomendación de viabilidad o no viabilidad económica de la solución basada en computación en la nube que atiende los requerimientos específicos formulados por la organización
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización 2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI 3. Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización 4. Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización 5. Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización 6. Recomendación de viabilidad o no viabilidad económica de la solución basada en computación en la nube que atiende los requerimientos específicos formulados por la organización	**7. SELECCIÓN DEL PROVEEDOR**	7. Proveedor Seleccionado
1. Contexto de Gobierno y Gestión de TI y los niveles de Gestión de Riesgo de la Organización 2. Elementos guías para explorar la adopción de la computación en la nube dentro de su contexto de gobierno y gestión de TI 3. Documento de requerimientos funcionales y no funcionales de la Solución específica basada en computación en la nube que busca la organización 4. Modelo de servicio y el modelo de despliegue de computación en la nube identificado para la solución específica buscada por la organización 5. Análisis de riesgos de la solución y modelo de servicio y despliegue seleccionado para atender los requerimientos formulados por la organización 6. Recomendación de viabilidad o no viabilidad económica de la solución basada en computación en la nube que atiende los requerimientos específicos formulados por la organización 7.Proveedor seleccionado	**8. CONTRATACIÓN**	8. Documento revisado que regule la relación de Cliente – proveedor para la prestación de la solución de computación en la nube

6. APLICACIÓN Y RESULTADOS OBTENIDOS

En el presente capítulo se aplicará parcialmente el marco metodológico propuesto, elementos de las fases 2, 3 y 8, a un caso particular teniendo como referencia una organización genérica.

Tanto en un escenario tradicional - con los activos de información en las instalaciones de la empresa -, como bajo un modelo de computación en la nube, hay requisitos que cumplir. Por ejemplo, el control de acceso a las aplicaciones es un requisito en ambos escenarios. En ambos escenarios hay riesgos, algunos comunes, otros en un escenario pero no en otro.

Se presentará inicialmente el caso de referencia y después se presentarán los factores de riesgos identificados para el modelo de servicio, Software como servicio SaaS (Fase 2 La organización en la nube: Identificación de riesgos), se traducirán esos factores de riesgos en requerimientos que apoyen tratamiento de ellos (Fase 3 Requerimientos) y se describirán elementos que se solicitarán al Departamento legal sean incluidos en las condiciones de contratación (entrada para Fase 8 Contratación)

Para la organización se tomó como referencia su Sistema de gestión de riesgos que contiene la librería de riesgos categorizados, el mapa de riesgos, las tablas de impacto. Además se revisaron riesgos específicos para la computación en la nube especificados por organismos como ENISA (European Network and information Security Agency), NIST (National Institute of Standards amd technology.) y Gartner.

6.1 CASO

Empresa XCV, fundada en Colombia, hace 20 años, pero con accionistas mayoritarios extranjeros. Cuenta con un equipo humano de 750 empleados distribuidos en oficinas en las principales ciudades de Colombia. La gerencia de TI está conformada por veinte funcionarios que ejecutan sus labores teniendo como referencia procesos fundamentados en COBIT e ITIL, que hacen parte del sistema de Gestión de calidad, el cual está certificado. El centro de cómputo está en la sede principal y se tiene un centro de datos contingente. Se está construyendo un plan de continuidad del negocio de la empresa. La empresa posee un plan estratégico que actualiza cada 4 años, la Gerencia de TI tiene un plan estratégico alineado con el corporativo. Existe una oficina central de administración del riesgo que coordina la gestión de riesgo en las diferentes dependencias, administra el inventario de riesgos de la compañía y mantiene el mapa de riesgo de la empresa. La compañía busca una solución de nómina en la nube bajo el modelo de servicio

Software como servicio (SaaS) que reemplace el sistema de nómina actual que tiene 20 años y que se ejecuta en los recursos de la empresa (on premise)

6.2 FACTORES DE RIESGOS / REQUERIMIENTOS / CONSIDERACIONES CONTRACTUALES

6.2.1 Migración hacia la nube

El paso del esquema actual hacia la computación en la Nube en caso de no realizarse correctamente puede conllevar a pérdida de datos, a la divulgación de datos a terceros y a impactar la continuidad de los procesos de negocio.

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- El proveedor debe especificar la metodología de migración de datos y suministrar un plan detallado de actividades junto con el cronograma o aceptar utilizar procedimiento de migración de datos de la organización
- La organización requiere que los datos a migrar deben ir cifrados

A nivel contractual la organización incluirá clausula para regular este tema:

- Migración. El Proveedor se compromete a cumplir con la metodología de migración, el plan y cronograma ofrecidos en la propuesta. En caso de no poseer metodología, debe cumplir el procedimiento de migración de datos de la organización. La propuesta y sus anexos y a metodología propia de la organización son parte integral del contrato.

6.2.2 Ubicación de los datos

Los activos de información están sujetos a regulaciones de los países donde están ubicados y tratados. La organización puede verse expuesta a sanciones legales debido al incumplimiento de leyes en algunos países, principalmente las leyes de protección de datos personales y de propiedad intelectual.

La organización puede verse impactada por el acceso de datos por parte de terceros por leyes específicas de los países donde estén ubicados los datos.

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- El proveedor debe indicar los países donde están ubicados los centros de datos

- El proveedor debe certificar el cumplimento de las regulaciones específicas de los países
- El proveedor debe suministrar certificaciones de Puerto seguro (Safe harbor) de sus instalaciones de centro de datos

A nivel contractual la organización incluirá clausulas para regular este tema:

- Clausula de responsabilidad por incumplimiento de regulaciones internacionales
- El proveedor se compromete al cumplimiento de las leyes colombianas relacionadas con datos personales
    - Ley Estatuaria 1266 de diciembre 31 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
    - Ley Estatuaria 1581 Octubre 17 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
    - Decreto 1377 del 27 de junio de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Cumplimiento de la directiva Europea 95/46 de protección de datos personales en caso de tener Centro de cómputos en Europa
- Limitación al Proveedor para mover los activos de información hacia ubicaciones que la organización no desea
- El proveedor se obliga a informar al Cliente cualquier cambio de ubicación de sus centros de datos

6.2.3 Localización del software

La organización se expone a incumplimientos de ley, sanciones debido a no incluir los requisitos de ley en la funcionalidad del software

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- El software debe incluir como estándar de producto los requerimientos legales de Colombia y su inclusión en los términos que exige la ley
- El proveedor debe cumplir el requisito de actualizar el software con las funcionalidades necesarias para cumplir las leyes de Colombia dentro de los términos normativos

A nivel contractual la organización incluirá clausulas para regular este tema:

- Compromiso del proveedor de asegurar que las localizaciones son parte integral y estándar del producto dentro de los términos establecidos por la ley
- Multas por no cumplir con los requisitos legales a tiempo

6.2.4 Propiedad de datos

La organización puede ver impactada la continuidad de sus operaciones y exponerse a divulgación de datos a terceros debido a la pérdida de propiedad de los datos.

En la invitación a presentar ofertas se incluyen los siguientes requisitos / condiciones:

- La propiedad de los datos antes, durante y después del contrato de prestación de servicios será del cliente

A nivel contractual la organización incluirá clausulas para regular este tema:

- Cláusula de Propiedad de los datos donde se deja constancia que los datos y de cualquier activo de información entregado por parte del cliente son propiedad del cliente
- Clausula de confidencialidad en la información

6.2.5 Retorno de datos al terminar contrato

La organización puede ver impactada la continuidad de sus operaciones y exponerse a divulgación de datos a terceros por no tener acceso a sus datos en caso de terminación del contrato.

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- En caso de terminación del contrato, el proveedor entregará los datos y activos de información al cliente en formatos estándares legibles como Base de datos Microsoft SQL Server, archivos planos u archivos de Excel.que no requieran del software del proveedor para ser consultados
- El proveedor debe mantener durante 90 días los datos o hasta que el cliente le informe de su eliminación.
- El proveedor debe suministrar las especificaciones técnicas y controles que aseguren que los datos sean eliminados incluyendo los medios de copias de respaldo

A nivel contractual la organización incluirá clausulas para regular este tema:

- Clausula de retorno de datos donde el proveedor se compromete a:

- Devolver los datos estructurados del cliente en base de datos Microsoft SQL Server 2008, archivos planos, archivos de Excel
- Documentación de las estructuras de datos devueltas
- Devolver los datos no estructurados del cliente en su formato original
- Mantener un respaldo de la información 90 días o hasta que el cliente le informe que puede eliminarla, lo que ocurra primero.
- Eliminar los datos suministrando las evidencias del procedimiento realizado para revisión de la organización.
- No cargar costos al cliente por esta actividad

6.2.6 Ambientes compartidos

Impacto en la divulgación de información a terceros debido al acceso no autorizado de terceros que comparten los servicios en la nube (Multitenant)

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- El proveedor debe indicar los controles que eviten que otras empresas que comparten los servicios accedan los datos de la organización.

A nivel contractual la organización incluirá clausulas para regular este tema:

- Las partes acuerdan quien puede acceder a la información de la organización
- El proveedor documentará los controles que protegen los activos de información del cliente
- El proveedor suministrará anualmente un reporte emitido por una entidad reconocida e independiente que de fe del cumplimiento de los controles para evitar el acceso de terceros que compartan los ambientes

6.2.7 No Disponibilidad

La organización puede ver impactada la continuidad de sus operaciones debido a la no disponibilidad de las aplicaciones y datos

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- La organización requiere una disponibilidad mensual del 99.999%
- Se requiere que el proveedor especifique el esquema de respaldo de información, las herramientas utilizadas y los controles para custodia de la información respaldada
- Se requiere un esquema de alta disponibilidad con transferencia inmediata de control entre los sitios principal y alterno
- El proveedor debe especificar su Plan de recuperación ante desastres o Plan de continuidad del negocio o certificación de un tercero de su implementación

- En caso de un desastre el proveedor debe cumplir como mínimo Tiempo Objetivo de recuperación de n horas.

A nivel contractual la organización incluirá clausulas para regular este tema:
- Disponibilidad: Definición, fórmula de cálculo y multas por incumplimiento
- Certificaciones: El proveedor debe poseer y mantener certificaciones de construcción y operación de los centros de cómputo actuales y futuros emitida por el uptime institute
- El proveedor se compromete a establecer y mantener un Plan de recuperación de desastres (DRP)
- El proveedor suministrará al cliente un reporte de una entidad reconocida donde se demuestre las pruebas exitosas de sus DRP /BCP.

6.2.8 Seguridad

La organización está expuesta a impactos económicos, legales, de cumplimiento, de continuidad en la operación, debido a la ocurrencia incidentes de seguridad.

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- El proveedor debe cumplir Modelo de seguridad de la organización (incluido en la invitación)
- El proveedor de servicios debe poseer certificación ISO 27001
- El proveedor debe suministrar el reporte de un tercero independiente , AICPA SSAE 16 SOC 2
- El proveedor debe suministrar si Modelo de seguridad o indicar su cumplimiento o no de los requisitos del modelo de seguridad de la empresa con certificaciones de entidades reconocidas de auditoría de seguridad
- El proveedor debe especificar el esquema de control de acceso y el sistema de Gestión de identidades que utiliza
- Los centros de cómputos del proveedor deben poseer nivel Tier 4 para Instalaciones construidas y Sostenibilidad de la operación, certificado por el Uptime Insttute

A nivel contractual la organización incluirá clausulas para regular este tema:
- Certificaciones: El proveedor se compromete a mantener la certificación ISO 27001 o norma equivalente que la sustituya. Cada año reportará el alcance y estado de certificación
- Certificaciones: El proveedor debe poseer y mantener certificaciones de construcción y operación de los centros de cómputos actuales y futuros emitida por el uptime institute. Cada año reportará el alcance y estado de certificación

- Reportes de terceros: El proveedor realizará evaluaciones de seguridad por entidades independientes reconocidas y entregará al cliente los resultados de las mismas.

6.2.9 Cumplimiento SOX

Impacto en la realización de objetivos corporativos e impacto económico debido al no cumplimiento de requisitos de auditoría y control.

En la invitación a presentar ofertas se incluyen los siguientes requisitos:

- El proveedor debe cumplir SOX (The Sarbanes–Oxley Act of 2002)

A nivel contractual la organización incluirá clausulas para regular este tema:

- El proveedor entregará un reporte de cumplimiento de los requisitos SOX cada año emitido por entidad competente independiente

6.2.10 Niveles de servicio

Las diferentes prestaciones informáticas tienen atributos y características, deberes y responsabilidades que conforman los acuerdos de niveles de servicio, que deben cumplirse para evitar exponer a la organización a diferentes tipos de impactos como Disponibilidad, Pérdidas económicas, Sanciones

En la invitación a presentar ofertas, se colocaron los valores mínimos esperados para cada atributo de servicio

En el contrato se incluyeron en forma clara las métricas, períodos de evaluación, forma de comunicación, penalizaciones por incumplimiento y por perjuicios ocasionados por los incumplimientos.

6.2.11 El contrato

La organización se expone a pérdidas económicas debido a la firma de contratos con condiciones desfavorables

Las empresas proveedores de servicios de computación en la nube ofrecen contratos de adhesión, con poca o nula flexibilidad con un clausulado que protege sus intereses.

Por otro lado la organización tiene modelos de contratos que protegen sus intereses y que han sido estructurados en el tiempo con base en la experiencia de adquirida. Por ser una contratación de bienes / servicios intangibles para los cuales no hay una normatividad, la empresa ha decidido contratar la asesoría jurídica para la revisión del contrato a establecer.

En la invitación a cotizar la organización incluirá su modelo de minuta de contratación con el objeto de regular la contratación con condiciones que son conocidas por el proponente con anticipación

A nivel contractual la organización incluirá clausulas para regular los siguientes temas:

- Forma de pago: Esquema de pago incluyendo el procedimiento para manejar los pagos regulares, deducciones por incumplimientos y el manejo de los pagos ante incumplimientos y terminaciones anticipados
- Tiempo de contratación: Busca regular los tiempos mínimos de contratación, condiciones de finalización y reglas de manejo ante finalizaciones anticipadas
- Reglas clara para aumentar / disminuir servicios y los costos asociados fijadas con anticipación
- Jurisdicción: La jurisdicción debe ser Barranquilla, Colombia.
- Solución de conflictos: Centro de Conciliación Cámara de Comercio de Barranquilla
- Incremento en los costos: Asociados a IPC de Colombia si los valores están en Pesos. Tasa de Inflación de USA si están en USD Dólares.

7. CONCLUSIONES

A continuación se presentan las conclusiones resultado de la realización del proyecto y teniendo como referencia los objetivos planteados.

- La computación en la nube es una alternativa tecnológica cuyo uso ha ido en aumento y con expectativas de crecimiento
- Al involucrar diferentes elementos tecnológicos y diferentes prestaciones informáticas, la adopción de la computación en la nube plantea retos para las dependencias de Tecnologías de la información: Seguridad, Riesgos, Cumplimiento, Continuidad del negocio, Cambio en el enfoque de inversiones y gastos, Gestión y gobierno de TI.
- Las organizaciones requieren de estrategias para implementar la Computación en la nube superar los retos y desafíos que ello implica
- Las organizaciones requieren acudir a las entidades reconocidas ampliamente para conocer, unificar y mantener actualizada la información y tendencias sobre la computación en la nube
- Las normas, estándares y mejores prácticas de gobierno y gestión de TI junto con las políticas, normas internas de la organización existentes, facilitan el camino hacia la nube
- El uso del marco metodológico desarrollado puede ayudar a las organizaciones a adoptar soluciones basadas en computación la nube dentro de un contexto de gestión y gobierno de TI

BIBLIOGRAFIA

BADGER, Lee, et al. Cloud computing Synopsis and recommendations . National Institute of Standards and technology. NIST Special publication 800-146. USA, Mayo 2012. 81p.

BORTNIK, Sebastián. La serie de normas ISO 27000. [en línea]. USA. Publicado el 16 de abril de 2010. Disponible en internet: http://www.welivesecurity.com/la-es/2010/04/16/la-serie-de-normas-iso-27000/

CLOUD SECURITY ALLIANCE. Security Guidance for critical areas of focus in cloud computing. Version 3.0. 2011. 177 p. . [en línea]. Disponible en: Internet

COMGROUP, inc. Request for proposal template Hosted/Cloud Unified Communications and collaboration solution. Marzo 2013. 36 p

COMGROUP, inc. Request for proposal template Hosted/Cloud Unified Communications and collaboration solution. Marzo 2013. 36 p

DIMENSION DATA.. IaaS Request for proposal template. Marzo 2, 2014. 24p

FARAHMAND, Fariborz. Risk perception and trust in cloud. Isaca Journal Volume 4, 2010. 8p

Forbes. Roundup Of Cloud Computing Forecasts And Market Estimates,2014. [en línea]. Disponible en: Internet: http://www.forbes.com/sites/louiscolumbus/2014/03/14/roundup-of-cloud-computing-forecasts-and-market-estimates-2014/

IBM. Moving from the backoffice to the front lines. [en línea]. Estados Unidos. 2013. Disponible en: Internet: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03580USEN 27 p

IDC. Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast (Doc #242464)" [en línea]. Disponible en: Internet: http://www.idc.com/getdoc.jsp?containerId=242464

IDC. Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast (Doc #242464 [en línea]. Disponible en: Internet: http://www.idc.com/getdoc.jsp?containerId=242464

Information Systems Audit and Control Foundation. Cobit Resumen Ejecutivo. Abril de 1998. 2da. Edición. 19p

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION (ICONTEC). Gestión del riesgo: Principios y Directrices. NTC-ISO 31000. Bogotá: El instituto, 2011. 12 p

IINTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. ISO 31000:2009 Risk Management: Principios and Guidelines: Abstract. [en línea]. Disponible en: Internet:: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170. 24 p

INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. ISO 31004:2013 Risk Management: Guidance for the implementation of ISO 31000: Abstract. [en línea]. Disponible en Internet: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56610 37p

INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. ISO Guidance 73:2009 Risk Management: Vocabulary: Abstract. [en línea]. Disponible en Internet: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44651 15 p.

INTERNATIONAL ORGANIZATION FOR STANDARDS. ISO Standards Catalogue. IEC 31010:2009 Risk Management: Risk Assessment techniques. [en línea]. Disponible en Internet: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51073 176 p

ISACA. Calcular el ROI de la nube: Desde la perspectiva del cliente. USA. Julio 2013. 17p

ISACA. COBIT® 5 Enabling Information.. United States of America, 2013.. 90 p. ISBN 978-1-60420-350-92

ISACA. COBIT® 5 for Assurance (Preview).. United States of America, 2013.. 16 p. ISBN 978-1-60420-340-0

ISACA. COBIT® 5 for information security (Preview). United States of America, 2012.. ISBN 978-1-60420-255-7

ISACA. COBIT® 5 for Risk (Preview).. United States of America, 2013.. 19 p. ISBN 978-1-60420-340-0

ISACA. COBIT® 5 Implementación. Quinta Edición. Estados Unidos, 2012. 28 p. ISBN 978-1-60420-289-2

ISACA. Controls and Assurance in the cloud: Using COBIT 5. United States of America, 2013.. 19 p.. ISBN 978-1-60420-465-0

ISACA. COBIT® 5 Procesos Catalizadores.. Quinta Edición. Estados Unidos, 2012. 230 p. ISBN 978-1-60420-285-4

ISACA. COBIT® 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Quinta Edición. Estados Unidos, 2012. 94 p. ISBN 978-1-60420-282-3

ISACA. Gobierno en la nube: Preguntas que los consejos directivos deben formular. 2013. 9 p

ISACA. Principios rectores para la adopción y el uso de la computación en la nube. Febrero, 2012. 16 P

ISACA. Security considerations for cloud computing. 2012. 80 p. ISBN 978-60420-263-2

ISO 27k timeline. [en línea]. Disponible en: Internet: http://www.iso27001security.com/ISO27k_timeline.gif.

KLU Cloud Computing Seminar. [En línea] India, KLU University, Disponible en internet: http://klucloudseminar.weebly.com/

Las empresas colombianas se suben a la nube. [en línea] disponible en internet: http://avanxo.com/estudio.html

MANN, Andi. MILNE Hurt. MORAIN Jeanne. How to calculate the advantages of a private cloud to make a business case. Searchcloudcomputing.com [En línea]. Disponible en internet http://www.bitpipe.com/detail/RES/1308681118_97.html 10p

MARSH. The cloud Risk framework: Informing decisions about moving to the cloud. United Kingdom. Mayo 2012. 20 p.

MELL, Peter. TIMOTHY Grance. US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, The NIST Definition of Cloud Computing, NIST,USA. 2011

NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY (NIST). Technical considerations for USG Cloud Computing deployment Decisions. Fisrt working draft. USA, Noviembre 3, 2001. 90p

Resultados del estudio nacional de tendencias de adopción de Cloud computing y nuevas tecnologías. 2013. . [en línea] disponible en internet: http://cintel.org.co/wp-content/uploads/2013/06/resultados-del-estudio.pdf

SCHAEFER. Thomas. HOFMANN, et al. Selecting the right cloud operating model: Privacy and Data Security in the Cloud. Vol. 3, 2014. ISACA Journal [En línea]. Disponible en internet: http://www.isaca.org/Journal/Past-Issues/2014/Volume-3/Documents/Selecting-the-Right-Cloud-Operating-Model_joa_Eng_0514.pdf

SOBRINOS, Roberto. Cobit Second Edition: Planificación y Gestión de Sistemas de Información. España. 19 de Mayo 1999. 66p

TAPPER, David. GENS, Frank. Prepare and Assess readness for cloud services. IDC..USA. Marzo 2011. 13 p,

The ISO Directory. A Short History of the ISO 27000 Standards. [En línea]. Disponible en internet: http://www.27000.org/thepast.htm

THE OPEN GROUP. Jericho Forum Cloud Cube Model. USA. Abril 2009. 16 p